PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Yoshihiko Takagi et al.
Serial No.:	10/782,556
Filed:	February 19, 2004
Title:	"MEMORY DEVICE"
Docket No.:	36462

LETTER

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Enclosed is a certified copy of Japan Patent Application No. 2003-042288, filed February 20, 2003; the priority of which has been claimed in the above-identified application.

Respectfully submitted,

PEARNE & GORDON LLP

Jeffrey J. Sopko, Reg. No. 27676

1801 East 9th Street
Suite 1200
Cleveland, Ohio 44114-3108
(216) 579-1700

March 16, 2004

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, Va. 22313-1450 on the date indicated below.

Jeffrey J. Sopko
Name of Attorney for Applicant(s)

03/16/2004
Date

Signature of Attorney

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月２０日

出願番号
Application Number: 特願２００３－０４２２８８

[ST. 10/C]: [ＪＰ２００３－０４２２８８]

出願人
Applicant(s): 松下電器産業株式会社

２００４年　２月　３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３００５５８７

【書類名】　特許願
【整理番号】　2030744066
【提出日】　平成15年 2月20日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 15/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　高木　佳彦
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　菊地　隆文
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100099254
　【弁理士】
　【氏名又は名称】　役　昌明
【選任した代理人】
　【識別番号】　100100918
　【弁理士】
　【氏名又は名称】　大橋　公治
【選任した代理人】
　【識別番号】　100105485
　【弁理士】
　【氏名又は名称】　平野　雅典

【選任した代理人】

【識別番号】　100108729

【弁理士】

【氏名又は名称】　林　紘樹

【手数料の表示】

【予納台帳番号】　037419

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9102150

【包括委任状番号】　9116348

【包括委任状番号】　9600935

【包括委任状番号】　9700485

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　メモリデバイス

【特許請求の範囲】

【請求項１】　電子機器から直接アクセスすることができない耐タンパー性の第１のメモリと、電子機器から直接アクセスすることができない非耐タンパー性の第２のメモリとを備え、前記第２のメモリを使用して、前記第１のメモリに蓄積されたデータを退避することを特徴とするメモリデバイス。

【請求項２】　退避するデータが、アプリケーションプログラムのインストール、または前記アプリケーションプログラムの実行によって生成されたデータであることを特徴とする請求項１に記載のメモリデバイス。

【請求項３】　前記データを退避するとき、アプリケーションプログラムのプログラムコードを廃棄することを特徴とする請求項２に記載のメモリデバイス。

【請求項４】　前記データを退避するとき、アプリケーションプログラムのプログラムコードを前記第１のメモリに残すことを特徴とする請求項２に記載のメモリデバイス。

【請求項５】　退避するデータが、アプリケーションプログラムのインストール、または前記アプリケーションプログラムの実行によって生成されたデータと、前記アプリケーションプログラムのプログラムコードとであることを特徴とする請求項１に記載のメモリデバイス。

【請求項６】　前記第１のメモリに蓄積されたデータの管理情報が格納された管理テーブルを具備し、前記管理情報に退避の可否を示す情報が含まれることを特徴とする請求項１に記載のメモリデバイス。

【請求項７】　前記アプリケーションプログラムは、前記第１のメモリにダウンロードされてインストール処理されたものであることを特徴とする請求項２または５に記載のメモリデバイス。

【請求項８】　前記アプリケーションプログラムは、前記第２のメモリにダウンロードされ、前記第１のメモリにインストール処理されたものであることを特徴とする請求項２または５に記載のメモリデバイス。

【請求項９】　前記アプリケーションプログラムは、前記第２のメモリにダウンロードされ、前記第２のメモリにインストール処理されたものであることを特徴とする請求項２または５に記載のメモリデバイス。

【請求項１０】　退避するデータとその署名情報とを暗号化した上で、退避することを特徴とする請求項１に記載のメモリデバイス。

【請求項１１】　退避した情報を管理する退避情報管理手段を前記第１のメモリ内に備え、退避するデータを暗号化して退避し、前記暗号化されたデータの署名情報を前記退避情報管理手段へ保存することを特徴とする請求項１に記載のメモリデバイス。

【請求項１２】　電子機器からの指示に基づいて退避するデータを決定することを特徴とする請求項１または６に記載のメモリデバイス。

【請求項１３】　前記第１のメモリへのアプリケーションプログラムのダウンロードまたはインストールの指示を受けた際に、前記第１のメモリにダウンロードまたはインストールを行う余地が無いとき、前記第１のメモリに蓄積された退避可能なデータから任意のデータを退避させることを特徴とする請求項１に記載のメモリデバイス。

【請求項１４】　電子機器からの復元指示により、退避した特定のデータを復元することを特徴とする請求項１または１２に記載のメモリデバイス。

【請求項１５】　電子機器からのアプリケーションプログラムの起動指示により、前記アプリケーションプログラムに関する退避データを復元することを特徴とする請求項１または１３に記載のメモリデバイス。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、半導体メモリカードなどのメモリデバイスに関し、特に、秘匿性を備えた領域の効率的な活用を可能にするものである。

【０００２】

【従来の技術】

近年、電子商取引などへの利用が拡大しているＩＣカードは、耐タンパー性の

モジュール内にメモリ領域を有しており、そのため、データを強固に秘匿することができ、複製や偽造に対して固い耐性を備えている。しかし、ＩＣカードのメモリ領域は、数十キロバイト程度の僅かなメモリ容量しか有していないため、多くのデータを格納することができない。

【０００３】

このＩＣカードに格納されたアプリケーションプログラム（以下、「ＡＰ」と言う）を一時的に端末に退避させて、ＩＣカードを有効に活用する技術が下記特許文献１に記載されている。このＩＣカードは、暗号化鍵を生成・管理し、退避対象のＡＰを暗号化してから端末に退避させる。また、退避させたＡＰを回復するときは、端末から受け取ったＡＰを、管理している暗号化鍵を用いて復号化し、ＩＣカード内部のメモリ領域に再格納する。

【０００４】

【特許文献１】

特開２０００－１１１０１号

【０００５】

【発明が解決しようとする課題】

しかし、ＩＣカードに格納したＡＰを端末Ａに退避させた場合は、その端末Ａ以外の端末ＢでＡＰを利用しようとすると、端末ＡをＩＣカードに接続して、退避させたＡＰをＩＣカード内部のメモリ領域に再格納し、その後に端末ＢとＩＣカードとを接続したり、あるいは、端末Ａに退避したＡＰを、ネットワーク等を介して端末Ｂに移送し、その後に端末ＢとＩＣカードとを接続したりする必要がある。つまり、ＡＰをＩＣカードの外に退避させた場合は、退避先の端末Ａ以外の端末ＢでＡＰを利用する場合に、極めて煩雑な手順が必要になるという問題点がある。

【０００６】

本発明は、こうした従来の問題点を解決するものであり、秘匿性を備えた領域を効率的に活用して、ＡＰの利用に必要な多くのデータを内部で安全に保持することができるメモリデバイスを提供することを目的としている。

【０００７】

【課題を解決するための手段】

そこで、本発明のメモリデバイスには、電子機器から直接アクセスすることができない耐タンパー性の第１のメモリと、電子機器から直接アクセスすることができない非耐タンパー性の第２のメモリとを設け、第２のメモリを使用して、第１のメモリに蓄積されたデータを退避するように構成している。

このメモリデバイスでは、多数のＡＰの利用に必要なデータをデバイス内部で安全に保持することができるため、認証条件を満たす端末であれば、どの端末でも、そこに保持されたデータを利用することができる。

【０００８】

【発明の実施の形態】

本発明の実施形態における半導体メモリカード（ここでは「セキュアメモリカード」と呼ぶことにする）は、図２の概念図に示すように、耐タンパー性モジュール（tamper resistant module:ＴＲＭ）４０に含まれる内部ＣＰＵ３０及び内部不揮発性メモリ４１と、非認証領域５３、認証領域５２及びセキュア領域５１を備える大容量不揮発性メモリ５０と、端末装置（リード／ライト（Ｒ／Ｗ）装置）の外部ＣＰＵ６０と通信して、端末装置によるメモリ領域へのアクセスを制御する制御部２０とを備えている。

【０００９】

内部不揮発性メモリ４１及びセキュア領域５１に対しては、内部ＣＰＵ３０のみがアクセス可能であり、端末装置は、内部不揮発性メモリ４１及びセキュア領域５１に直接アクセスすることはできない。また、制御部２０は、端末装置の認証処理を行い、認証した外部ＣＰＵ６０が認証領域５２にアクセスすることを許可する。一方、非認証領域５３に対しては、端末装置は無条件でアクセスすることができる。

【００１０】

ＴＲＭ４０の不揮発性メモリ４１は、例えば、１６バイト単位で消去・書き込みができるＥＥＰＲＯＭから成り、また、大容量不揮発性メモリ５０は、例えば、５１２バイト等のブロック単位での消去と１バイト単位での書き込みとが可能なフラッシュメモリから成る。

外部ＣＰＵ６０は、非認証領域５３に無条件でアクセスすることができ、また、認証領域５２には、制御部２０での認証を済ませた場合にアクセスすることができるが、セキュア領域５１及び内部不揮発性メモリ４１の存在を知ることはできず、これらに直接アクセスすることはできない。

【００１１】

セキュア領域５１及び内部不揮発性メモリ４１に対しては、内部ＣＰＵ３０だけがアクセス可能である。セキュア領域５１と内部不揮発性メモリ４１との違いは、内部不揮発性メモリ４１がＴＲＭ４０に設けられているのに対し、セキュア領域５１が、耐タンパー性を持たない大容量不揮発性メモリ５３に設けられている点である。そのため、セキュア領域５１は、内部不揮発性メモリ４１に比べて大きい蓄積容量を持つことができる。その反面、セキュリティレベルは、ＴＲＭ４０に設けられた内部不揮発性メモリ４１よりも低い。この４つの領域のセキュリティレベルは、非認証領域５３が最も低く、認証領域５２、セキュア領域５１、内部不揮発性メモリ４１の順に高くなっている。

【００１２】

図３のブロック図は、セキュアメモリカード１０の構成を示している。セキュアメモリカード１０は、大別して、制御部２０と、大容量不揮発性メモリ５０と、図２のＴＲＭ４０に相当するＩＣ部１１とで構成される。大容量不揮発性メモリ５０は、非認証領域５３と、認証領域５２と、セキュア領域５１と、これらの領域のアドレス情報が格納されたアドレス情報管理領域５４とを有している。

【００１３】

制御部２０は、Ｒ／Ｗ装置６９との間でデータの授受を行うデータＩ／Ｆ部２１と、Ｒ／Ｗ装置６９との間でコマンドの授受を行うコマンドＩ／Ｆ部２２と、Ｒ／Ｗ装置６９を認証する制御認証部２３と、受け付けたコマンドを解釈してコマンドに応じた処理を行う制御コマンド処理部２４と、大容量不揮発性メモリ５０へのアクセスを制御するとともにＩＣ部１１とのデータの受け渡し窓口となるアクセス制御部２５と、大容量不揮発性メモリ５０との間でデータを受け渡す大容量不揮発性メモリＩ／Ｆ部２６とを備えている。

【００１４】

また、耐タンパー性のＩＣ部１１は、内部不揮発性メモリ４１と、制御部２０との間でデータやコマンドの授受を行うＩ／Ｆ部１２と、コマンドを解釈してコマンドに応じた処理を行うＩＣコマンド処理部１３と、内部不揮発性メモリ４１及びセキュア領域５１にファイル形式で格納されたデータを管理するファイル管理部１４と、Ｒ／Ｗ装置６９を認証し、認証したＲ／Ｗ装置６９に対して内部不揮発性メモリ４１及びセキュア領域５１へのデータアクセスを許可するＩＣ認証部１５と、内部不揮発性メモリ４１及びセキュア領域５１への書き込み／読み出しデータに対して内部不揮発性メモリ４１に格納された鍵を用いて暗号化／復号化を行う暗復号回路１７と、内部不揮発性メモリ４１及びセキュア領域５１の管理を行うメモリ管理部１６と、内部不揮発性メモリ４１へのデータの授受を行う内部不揮発性メモリＩ／Ｆ部１８とを備えている。

【００１５】

制御部２０の制御コマンド処理部２４は、Ｒ／Ｗ装置６９から受信したコマンドを解釈し、そのコマンドが

・大容量不揮発性メモリ５０の認証領域５２または非認証領域５３へのアクセスを要求するものであるか、

・認証を要求するものであるか、

・ＩＣ部１１による処理を要求するものであるか

を判断し、大容量不揮発性メモリ５０の認証領域５２または非認証領域５３へのアクセスを要求しているときは、アクセス制御部２５に大容量不揮発性メモリ５０へのアクセス制御を指示し、ＩＣ部１１による処理を要求しているときは、アクセス制御部２５にＩＣ部１１へのコマンドの転送を指示し、また、認証を要求しているときは、制御認証部２３に認証処理を指示する。

【００１６】

アクセス制御部２５は、大容量不揮発性メモリ５０へのアクセス制御に当たって、大容量不揮発性メモリ５０のアドレス情報管理領域５４に記録されたアドレス情報を参照する。端末（Ｒ／Ｗ装置６９）が大容量不揮発性メモリ５０の論理アドレスを指定してアクセスを求めて来たときは、アドレス情報管理領域５４の記録から、指定されたアドレスが大容量不揮発性メモリ５０のいずれの領域に属

しているかを判断し、認証領域５２へのアクセス要求に対しては、認証済み端末に限って許可する。

【００１７】

また、ＩＣ部１１のＩＣコマンド処理部１３は、制御部２０から送信されたコマンドを解釈し、その処理要求が、

・内部不揮発性メモリ４１へのデータ書き込み／読み出しを要求するものであるか、

・セキュア領域５１へのデータ書き込み／読み出しを要求するものであるか、

・認証を要求するものであるか、

・その他の処理を要求するものであるか

を判断する。

【００１８】

コマンドが、認証を要求しているときには、ＩＣコマンド処理部１３は、ＩＣ認証部１５にＲ／Ｗ装置６９の認証処理を指示する。

また、コマンドが、内部不揮発性メモリ４１へのデータの書き込み／読み出し、または、セキュア領域５１へのデータの書き込み／読み出しを要求するコマンドであるときには、ＩＣコマンド処理部１３は、ＩＣ認証部１５において認証処理が済んでいるかを確認し、認証処理が済んでいる場合は、その要求を許可し、その要求が書き込み要求であるときは、書き込むデータを、格納先の情報を付してメモリ管理部１６に送る。

【００１９】

内部不揮発性メモリ４１及びセキュア領域５１を管理するメモリ管理部１６は、書き込むデータを暗復号回路１７で暗号化し、データに署名（この処理に用いる暗号鍵や検証鍵は内部不揮発性メモリ４１に格納されている）を付した後、内部不揮発性メモリ４１に書き込むべきデータを、内部不揮発性メモリＩ／Ｆ部１８を介して、内部不揮発性メモリ４１に書き込み、書き込み位置の情報をファイル管理部１４に伝える。また、セキュア領域５１に書き込むべきデータを、大容量不揮発性メモリＩ／Ｆ部２６を介して、大容量不揮発性メモリ５０のセキュア領域５１に書き込み、書き込み位置の情報をファイル管理部１４に伝える。なお

、署名は、暗号化したデータとは別に内部不揮発性メモリ４１で保持する場合もある。

【００２０】

ファイル管理部１４は、メモリ管理部１６から伝えられた情報を基に、内部不揮発性メモリ４１及びセキュア領域５１に格納されたファイルを管理する。

また、ＩＣコマンド処理部１３は、その要求が読み出し要求であるときは、読み出すべきデータのファイル位置をファイル管理部１４に求め、メモリ管理部１６にそのファイルの読み出しを要求する。

メモリ管理部１６は、そのファイルを内部不揮発性メモリ４１またはセキュア領域５１から読み出すと、暗復号回路１７でデータの署名検証や復号化を行い、ＩＣコマンド処理部１３に送る。

【００２１】

復号化されたデータは、制御部２０に送られ、データＩ／Ｆ部２１からＲ／Ｗ装置６９に送信される。

また、ＩＣコマンド処理部１３は、メモリ容量が少ない内部不揮発性メモリ４１を有効に活用するため、内部不揮発性メモリ４１に格納したデータをセキュア領域５１に退避させる処理を行う。以下、この退避処理について詳しく説明する。

【００２２】

（第１の実施形態）

ＩＣコマンド処理部１３は、端末から、セキュアカード内部で動作する、退避可能なＡＰのダウンロード（以下「ＤＬ」と言う）が要求された場合に、内部不揮発性メモリ４１に空きが有るときは、端末から送られたＡＰのプログラムコード（プログラムを記述するプログラムデータ）を内部不揮発性メモリ４１に格納する処理、即ち、ＤＬ処理を行う。また、端末のインストール要求に応じて、ＤＬしたＡＰのプログラムコードを実行し、ＡＰ用のデータを作成してＡＰを実行可能な状態にする処理、即ち、インストール処理を行う。

【００２３】

また、ＩＣコマンド処理部１３は、内部不揮発性メモリ４１に空きが無いとき

は、端末からの指示により（または、自らの判断で）、内部不揮発性メモリ４１に既に格納されている、退避可能なＡＰのプログラムコード及びデータをセキュア領域５１に退避させる処理を行い、空きができた内部不揮発性メモリ４１に、端末から送られたＡＰのＤＬ処理及びインストール処理を行う。

また、ＩＣコマンド処理部１３は、セキュア領域５１に退避したＡＰの起動が端末から要求された場合に、そのＡＰをインストール状態に戻すために、内部不揮発性メモリ４１に空いた領域が有るときは、起動要求されたＡＰのプログラムコード及びデータを内部不揮発性メモリ４１に復元（データ移動）し、そのＡＰを起動する。

【００２４】

この場合、内部不揮発性メモリ４１に空いた領域が無いときは、内部不揮発性メモリ４１に格納されている退避可能なＡＰのプログラムコード及びデータをセキュア領域５１に退避させ、空きができた内部不揮発性メモリ４１に、起動要求されたＡＰのプログラムコード及びデータを復元する。

なお、セキュア領域５１への退避は、ＡＰのインストール処理で作成したデータだけを対象に行い、ＡＰのプログラムコードについては内部不揮発性メモリ４１から削除するようにしても良い。プログラムコード自体は、退避するデータと違って、セキュアカードで生成したものではなく、いつでも端末から同じものをＤＬすることが可能なためである。このＡＰの起動は、セキュア領域５１に退避したＡＰのデータを内部不揮発性メモリ４１の空き領域に復元し、端末からＡＰのプログラムコードを内部不揮発性メモリ４１にＤＬして行われる。

【００２５】

図１は、この内部不揮発性メモリ４１の構成を示している。内部不揮発性メモリ４１の内部には、ＡＰのプログラムコードが格納されるＡＰ格納領域４１１と、ＡＰで利用するデータが格納されるデータ格納領域４１２と、内部不揮発性メモリ４１にプログラムコード及びデータが格納されたＡＰを管理するためのＡＰ管理テーブル４１３と、セキュア領域５１に退避したＡＰを管理するための退避ＡＰ管理テーブル４１４と、退避・復元するコードやデータの暗号化・復号化に用いる鍵と署名生成・検証に用いる鍵とが格納された鍵管理領域４１５とが設け

られている。

【００２６】

ＡＰ管理テーブル４１３には、図４に示すように、ＡＰがどのようなものであるかを一意に示すＡＰ識別子と、そのＡＰのインストール処理がされているか否かを示すインストールフラグと、プログラムコードが格納されたＡＰ格納領域４１１のアドレスを示すコードアドレスと、データが格納されたデータ格納領域４１２のアドレスを示すデータアドレスと、このＡＰが退避可能であるか否かを示す退避可否とが記述される。なお、退避可否は、ＡＰのＤＬ時に端末から伝えられる。

【００２７】

また、退避ＡＰ管理テーブル４１４には、図５に示すように、ＡＰ識別子と、退避させたデータの格納位置等を一意に特定するための退避データ識別子と、退避データに対する署名データとが記述される。退避データ識別子は、様々な形式で設定することができ、例えば（退避先アドレス＋データサイズ）を退避データ識別子としても良い。

また、図６には、退避データを格納するデータ退避領域５１１を備えたセキュア領域５１の構成を示している。

【００２８】

次に、ＡＰのＤＬ、インストール、退避、及び復元に伴うＡＰ管理テーブル４１３や退避ＡＰ管理テーブル４１４の遷移について説明する。

図１３（ａ）には、初期状態（ＡＰが１つもＤＬ／インストール／退避／復元されていない状態）のＡＰ管理テーブル４１３を示し、また、図１６（ａ）には、初期情報の退避ＡＰ管理テーブル４１４を示している。端末からＡＰとして退避可否が可のＡＰ１がＤＬされると、ＡＰ管理テーブル４１３には、図１３（ｂ）のように記述される。「ｃｏｄｅ１」は、ＡＰ格納領域４１１に格納されたＡＰ１のプログラムコードのアドレスを示している。さらに、退避可否が可のＡＰ２がＤＬされると、ＡＰ管理テーブル４１３の記述は図１３（ｃ）のようになる。ＡＰ１及びＡＰ２をインストールした状態では、ＡＰ管理テーブル４１３の記述は図１４（ｄ）のように変わり、データ格納領域４１２に格納されたＡＰ１の

データのアドレスが「ｄａｔａ１」として、データ格納領域４１２に格納されたＡＰ２のデータのアドレスが「ｄａｔａ２」として記述される。

【００２９】

図１４（ｅ）には、さらに、端末から退避可否が否のＡＰ３、退避可否が可のＡＰ４及びＡＰ５がＤＬされ、インストールした状態を示している。また、このときの内部不揮発性メモリ４１のＡＰ格納領域４１１及びデータ格納領域４１２の状態を図１７（ａ）に、セキュア領域５１のデータ退避領域５１１の状態を図１７（ｂ）に示している。ＡＰ格納領域４１１には空きが無い。

次に、このようにＡＰ格納領域４１１に空きが無い状態で、端末があるＡＰ（ここではＡＰ６）のＤＬを要求した場合には、端末とＩＣコマンド処理部１３との間で図７に示す処理が行われる。

【００３０】

端末がＡＰ６のＤＬを要求すると（①）、ＩＣコマンド処理部１３は、内部不揮発性メモリ４１のＡＰ格納領域４１１に空きが存在しないため、空き領域がない旨のエラー通知を端末に対して行う（②）。端末は、退避可能なＡＰ一覧を要求し（③）、カードから退避可能なＡＰ一覧を取得して（④）、その中から退避可能なＡＰ（ここではＡＰ２）を選択して、ＡＰ２の退避を要求する（⑤）。ＩＣコマンド処理部１３は、ＡＰ２の退避処理を行い（⑥）、退避完了通知を端末に伝える（⑦）。ＡＰ２の退避処理が行われた状態でのＡＰ管理テーブル４１３を図１５（ｆ）に示し、退避ＡＰ管理テーブル４１４を図１６（ｂ）に示し、また、内部不揮発性メモリ４１のＡＰ格納領域４１１及びデータ格納領域４１２の状態を図１８（ａ）に、セキュア領域５１のデータ退避領域５１１の状態を図１８（ｂ）に示している。

【００３１】

端末はＡＰ６のＤＬを要求し（⑧）、ＩＣコマンド処理部１３は、ＡＰ６のＤＬ処理を行い（⑨）、ＤＬ完了通知を端末に送る（10）。ＡＰ６のＤＬ処理が行われた状態でのＡＰ管理テーブル４１３を図１５（ｇ）に示し（アドレスｃｏｄｅ６は、ＡＰ２の退避により空き領域となったｃｏｄｅ２またはｄａｔａ２と同一となることもあるし、ならないこともある）、また、内部不揮発性メモリ４１

のＡＰ格納領域４１１及びデータ格納領域４１２の状態を図２０（ａ）に示している。

【００３２】

なお、ここでは、ＩＣコマンド処理部１３が端末からのＡＰ退避要求を待って退避処理を行う場合について示したが、ＡＰ格納領域４１１に空きが無いときに、ＩＣコマンド処理部１３が自ら判断してＡＰの退避処理を行うことも可能である。この場合、図８に示すように、端末がＡＰ６のＤＬを要求すると（①）、ＩＣコマンド処理部１３が、退避可能なＡＰの中から選択したＡＰ２を退避させて（②）、ＡＰ格納領域４１１に空き領域を確保した後、ＡＰ６のＤＬ処理を行い（③）、ＤＬ完了通知を端末に送る（④）、と言う処理手順になる。

このように、端末に意識されること無く、自動的に退避処理が行われる。また、この場合、ＡＰ６のＤＬ完了後、ＡＰ２を自動的に退避させたことを端末に通知するようにしても良い。

【００３３】

また、図７の⑥、あるいは、図８の②でのＡＰ退避処理は、図９（ａ）または図９（ｂ）に示す手順で実行される。図９（ａ）は、署名データをセキュア領域５１に格納する方式であり、まず、署名鍵を用いて、退避用データ（前述するように、インストール処理されたＡＰのプログラムコードと生成データとを退避用データにする場合と、生成データだけを退避用データにする場合とがある）の署名データを生成し（①）、退避用データと署名データとを連結し（②）、連結したデータを退避用暗号鍵で暗号化し（③）、暗号化したデータをセキュア領域５１のデータ退避領域５１１に格納する（④）。そして、退避ＡＰ管理テーブル４１４にＡＰ識別子及び退避データ識別子を追加する（この方式の場合には、署名データは、退避ＡＰ管理テーブル４１４に加えない）。インストール処理で生成したデータだけを退避用データとした場合は、ＡＰ格納領域４１１から退避対象ＡＰのプログラムコードを削除し、ＡＰ管理テーブル４１３上から退避対象ＡＰに関する情報を削除する。

【００３４】

一方、図９（ｂ）は、署名データを退避ＡＰ管理テーブル４１４に保存する方

式であり、退避用データを暗号鍵で暗号化し（①）、署名鍵を用いて暗号化データの署名データを生成し、この署名データを退避ＡＰ管理テーブル４１４に保存する（②）。暗号化したデータはセキュア領域５１のデータ退避領域５１１に格納する（③）。そして、退避ＡＰ管理テーブル４１４に、さらにＡＰ識別子及び退避データ識別子を追加する。インストール処理で生成したデータだけを退避用データとした場合は、ＡＰ格納領域４１１から退避対象ＡＰのプログラムコードを削除し、ＡＰ管理テーブル４１３上から退避対象ＡＰに関する情報を削除する。

【００３５】

次に、端末が、退避状態のＡＰ２に対して起動要求した場合のセキュアカード１０の動作について説明する。この場合、ＡＰ２が退避されていることを端末が認識し、端末からＡＰ２の復元要求を行う方法と、ＩＣコマンド処理部１３が、起動要求されたＡＰ２の退避を認識し、自らＡＰ２の復元処理を行う方法とがある。

【００３６】

図１０には、端末からＡＰ２の復元要求を行う場合の手順を示している。端末はＡＰ２の起動要求をセキュアカード１０に対して行う（①）。ＩＣコマンド処理部１３は、ＡＰ管理テーブル４１３を参照してＡＰ２が内部不揮発性メモリ４１に存在しないことを認識し（②）、端末にＡＰ２が内部不揮発性メモリ４１に存在しないことを通知する（③）。端末はセキュアカード１０に「退避ＡＰ管理テーブル」４１４の取得を要求し（④）、ＩＣコマンド処理部１３は、端末に退避ＡＰ管理テーブル４１４を送信する（⑤）。端末は退避ＡＰ管理テーブルによってＡＰ２が退避されていることを認識し、セキュアカード１０に任意のＡＰ（ここではＡＰ４）の退避要求を行う（⑥）。ＩＣコマンド処理部１３は、ＡＰ４の退避処理を行い（⑦）、端末に退避完了を通知する（⑧）。

【００３７】

図１９には、図２０の状態からＡＰ４を退避させたときのＡＰ格納領域４１１、データ格納領域４１２及びデータ退避領域５１１の状態を示し、また、図１６（ｃ）には、このときの退避ＡＰ管理テーブル４１４を示している。

次いで、端末はセキュアカード１０にＡＰ２の復元要求を行う（⑨）。ＩＣコマンド処理部１３は、ＡＰ２の復元処理を行い（10）、端末に復元完了を通知する（11）。図１５（ｈ）は、ＡＰ２を復元処理した状態のＡＰ管理テーブル４１３を示し（アドレスｃｏｄｅ７及びｄａｔａ７は、ＡＰ４の退避により空き領域となったｃｏｄｅ４またはｄａｔａ４と同一となることもあるし、ならないこともある）、また、図１６（ｄ）は、このときの退避ＡＰ管理テーブル４１４を示し、図２１は、このときのＡＰ格納領域４１１、データ格納領域４１２及びデータ退避領域５１１の状態を示している。

次いで、端末はセキュアカード１０に再度ＡＰ２の起動要求を行う（12）。ＩＣコマンド処理部１３は、ＡＰ２を起動し（13）、端末に起動完了を通知する（14）。

【００３８】

なお、③の通知において、同時に、ＡＰ２が退避中であることを通知することによって、④、⑤を省略することもできる。また、ＡＰ２が退避中であることを端末が認識している場合には、④以降の手順が行われる。また、ＡＰ２の退避がインストール処理で生成されたデータについてのみ行われ、ＡＰ２のプログラムコードが削除されている場合には、端末は、⑨の手順でＡＰ２のプログラムコードをＤＬする。

【００３９】

一方、図１１は、ＩＣコマンド処理部１３が、起動要求されたＡＰ２の退避を認識し、自らＡＰ２の復元処理を行う場合の手順を示している。端末はＡＰ２の起動要求をセキュアカード１０に対して行う（①）。ＩＣコマンド処理部１３は、ＡＰ管理テーブル４１３を参照してＡＰ２が内部不揮発性メモリ４１に存在しないことを認識し、次に、退避ＡＰ管理テーブル４１４を参照してＡＰ２が退避されていることを認識し、あるＡＰを退避対象として選択し（ここではＡＰ４）、その退避処理を行う。次いで、空いた領域にＡＰ２を復元し（②）、ＡＰ２を起動して（③）、端末には起動完了を通知する（④）。

【００４０】

この場合、ＡＰ２が退避されていることを気付いていない端末が、ＡＰ２の起

動指示を出した場合でも、そのＡＰ２を起動するための処理が、ＩＣコマンド処理部１３によって行われる。そのため、端末は、起動要求するＡＰが退避されているか否かを意識する必要がない。

なお、この方法は、ＡＰ２の退避がインストール処理で生成されたデータについてのみ行われ、ＡＰ２のプログラムコードが削除されている場合には、適用できない。

【００４１】

また、図１０の（10）、あるいは、図１１の②での復元処理は、退避処理が図９（ａ）の手順で行われているときは、図１２（ａ）の手順で、また、退避処理が図９（ｂ）の手順で行われているときは、図１２（ｂ）の手順で行われる。図１２（ａ）では、退避ＡＰ管理テーブル４１４のＡＰ識別子により退避データ（暗号化データ）を認識し、復号鍵を用いて暗号化データを内部不揮発性メモリ４１上に復号化する（①）。次いで、復号化したデータから退避データ本体と署名データとを認識し、検証鍵を用いて、署名データの正当性を検証する。署名が正当であるときは、退避用データ本体に含まれるプログラムコードを内部不揮発性メモリ４１のＡＰ格納領域４１１に、データをデータ格納領域４１２に復元する（②）。また、ＡＰ管理テーブル４１３にＡＰ識別子を記述し、インストールフラグをＯＮに設定し、ＡＰ格納領域４１１及びデータ格納領域４１２に格納した復元データのアドレスをコードアドレス及びデータアドレスとして記述する。最後にセキュア領域５１内の退避暗号化データと、退避ＡＰ管理テーブル４１４の当該ＡＰに関する部分を削除する。

【００４２】

また、図１２（ｂ）の手順では、退避ＡＰ管理テーブル４１４のＡＰ識別子により退避データ（暗号化データ）を認識し、検証鍵を用いて、退避ＡＰ管理テーブル４１４に記述された署名データとの検証を行う（①）。検証結果が正常であれば、復号鍵を用いて暗号化データを内部不揮発性メモリ４１上に復号化し（②）、プログラムコードを内部不揮発性メモリ４１のＡＰ格納領域４１１に、また、データをデータ格納領域４１２に復元する（③）。その後の処理は図１２（ａ）の場合と同じである。

【００４３】

また、ＡＰの退避がインストール処理で生成されたデータについてのみ行われている場合には、端末がＡＰのプログラムコードをＤＬしたときに、データの復元処理が次の手順で行われる。

復元対象ＡＰを端末からＤＬする。ＩＣコマンド処理部１３は、ＡＰ管理テーブル４１３にＡＰ識別子及びコードアドレスを記述し、ＤＬしたＡＰと同一のＡＰ識別子を退避ＡＰ管理テーブル４１４より検索する。対応するものが存在すれば、セキュア領域５１のデータ退避領域５１１から暗号化データを読み出し、復号化する。復号化したデータから、退避データ本体と署名データとを認識し、署名データの正当性の検証を行う。検証結果が正当であれば、退避データ本体を内部不揮発性メモリのデータ格納領域４１２に格納し、ＡＰ管理テーブル内の該当するＡＰのインストールフラグをＯＮに設定し、データアドレスとして、復元データを格納したデータ格納領域４１２のアドレスを設定する。最後にセキュア領域内の退避暗号化データと、退避ＡＰ管理テーブルの該ＡＰに関する部分を削除する。

【００４４】

ここでは、ＡＰのプログラムコードと、インストール処理で生成されたデータとを共に退避する場合、及び、データのみを退避し、プログラムコードを削除する場合について説明したが、プログラムコードに比べてデータのデータ量が遥かに大きい場合には、データのみをセキュア領域５１に退避し、プログラムコードは、内部不揮発性メモリ４１のＡＰ格納領域４１１に残しておくことも可能である。こうした方式を採ると、図１８に示すＡＰ格納領域４１１、データ格納領域４１２及びデータ退避領域５１１の状態は、図２２のように変わり、また、図２０に示す状態は、図２３のように変わる。

【００４５】

ＡＰのプログラムコード及びデータを共に退避する場合、並びに、データを退避し、プログラムコードを内部不揮発性メモリに残す場合には、図１１に示す、ＩＣコマンド処理部による自動的な復元処理手順が可能となる。

また、端末から、セキュア領域５１に退避中のＡＰの起動が要求されたとき、

次の手順により、ＡＰのプログラムコードやデータをセキュア領域５１に置いたまま、ＡＰの実行を行うことも可能である。

【００４６】

例えば、図１８、図１５（ｆ）及び図１６（ｂ）の状態にあるとき、端末がセキュアカード１０に対しＡＰ２の実行を要求すると、ＩＣコマンド処理部１３は、ＡＰ管理テーブル（図１５（ｆ））よりＡＰ２がインストール状態でないことを認識し、退避ＡＰ管理テーブル（図１６（ｂ））より退避中であることを認識し、退避データ識別子により、ｅｖａｃ２を読み出し、復号化と署名検証とを行う。署名検証が正常に終了すると、復号化データよりＡＰ２のプログラムコードを取得し、ＡＰ２の実行を行う。

この場合には、退避中のＡＰを内部不揮発性メモリ４１に復元することを要しない。

【００４７】

このように第１の実施形態のセキュアメモリでは、内部不揮発性メモリにＤＬされてインストール処理されたＡＰの内、退避の可能なものだけが退避される。そのため、最高度の機密を要するＡＰは、「退避不可」とすることにより、退避の対象から外れることができる。また、紛失の危険性を甘受できる程度のセキュリティを要求するＡＰは、「退避可」とすることにより、セキュアメモリにおける秘匿領域の効率的な利用が可能になる。

【００４８】

（第２の実施形態）

本発明の第２の実施形態におけるセキュアメモリの構成は、第１の実施形態（図２、図３）と同じである。

第１の実施形態では、ＡＰをセキュアメモリ１０の内部不揮発性メモリ４１にＤＬし、内部不揮発性メモリ４１に新たなＡＰをＤＬする空きが無いときに、インストール処理された退避可のＡＰを内部不揮発性メモリ４１からセキュア領域５１に退避させる場合について説明したが、第２の実施形態では、セキュア領域５１をＡＰのＤＬ先とすることを可能にしている。ただし、セキュア領域５１にＤＬされたＡＰのインストール処理は、内部不揮発性メモリ４１で行われる。

【００４９】

ＡＰのＤＬ先を内部不揮発性メモリ４１とするか、セキュア領域５１とするかは、次のような方式で決定される。

第１の方式では、ＤＬ時に、ＡＰのプログラムコードと合わせて、端末から内部不揮発性メモリＤＬ専用フラグを送信する。セキュアメモリ１０のＩＣコマンド処理部１３は、そのフラグを参照し、内部不揮発性メモリＤＬ指定がなされていれば、必ず内部不揮発性メモリ４１にＤＬし、内部不揮発性メモリＤＬ指定がなされていなければ、内部不揮発性メモリ４１に空きがあるときは、内部不揮発性メモリ４１にＤＬし、内部不揮発性メモリ４１に空きが無いときは、セキュア領域５１にＤＬする。

【００５０】

また、第２の方式では、端末がセキュア領域５１へのＤＬを許可する場合のみ、ＤＬ時にＡＰのプログラムコードと合わせて、セキュア領域ＤＬ許可フラグを送信する。セキュアメモリ１０のＩＣコマンド処理部１３は、セキュア領域ＤＬ許可フラグが付加されていれば、内部不揮発性メモリ４１に空きがあるときは、内部不揮発性メモリ４１に、内部不揮発性メモリ４１に空きが無いときは、セキュア領域５１にＤＬし、セキュア領域ＤＬ許可フラグが付加されていなければ、必ず内部不揮発性メモリ４１にＤＬする。

このセキュアメモリ１０のセキュア領域５１は、図２４に示すように、データ退避領域５１１の他に、ＤＬされたＡＰのプラグラムコードを格納するＡＰ保存領域５１２を備えている。

【００５１】

また、内部不揮発性メモリ４１は、図１と同様の構成を備えている。ただし、ＡＰ管理テーブルは、図２５に示すように、内部不揮発性メモリ４１にＤＬまたはインストールされた状態のＡＰを管理するためのＡＰ管理テーブル４１３と、セキュア領域５１にＤＬされたＡＰを管理するためのセキュア領域ＤＬＡＰ管理テーブル４１６とから成る。セキュア領域ＤＬＡＰ管理テーブル４１６には、ＡＰを内部不揮発性メモリ４１上でインストールするために必要となる事項、即ち、ＡＰが格納されているセキュア領域５１上の位置を示す「格納アドレス」、そ

のＡＰの改ざんの有無を確認するための「署名データ」、そのＡＰがインストール後に退避可能か否かを示す「退避可否フラグ」がＡＰ識別子と共に記述される。

【００５２】

ＡＰ管理テーブル４１３の項目は、第１の実施形態（図４）と同じであり、内部不揮発性メモリ４１上に格納されたＡＰが、インストール状態であるか否かを示す「インストールフラグ」、退避可能か否かを示す「退避可否フラグ」、インストール状態であるときのデータの所在を示す「データアドレス」、及び、プログラムコードの読み出し先を示す「コードアドレス」がＡＰ識別子と共に記述される。

【００５３】

このＡＰ管理テーブル４１３の特定番号、例えば＃４及び＃５は、セキュア領域５１にＤＬされたＡＰ（セキュア領域ＤＬＡＰ）のインストール用に確保されており、内部不揮発性メモリ４１へのＡＰのＤＬには、そこを使用することができない。そのため、内部不揮発性メモリ４１にＤＬするＡＰのＤＬ及びインストール処理は、ＡＰ管理テーブル４１３の＃１～＃３を使って、第１の実施形態と同じように行われる。

【００５４】

一方、セキュア領域５１にＤＬしたＡＰに対して、ＩＣコマンド処理部１３は、次の手順でインストールを行う。

セキュア領域ＤＬＡＰ管理テーブル４１６の格納アドレスにしたがって、セキュア領域５１のＡＰ保存領域５１２からＡＰのプログラムコードを読み出し、復号化及び署名検証を行う。検証結果が正常であれば、復号化したプログラムコードを内部不揮発性メモリ４１のＡＰ格納領域４１１に格納し、ＡＰ管理テーブル４１３のセキュア領域ＤＬＡＰ用の特定番号にＡＰ識別子、コードアドレス、退避可否フラグ（セキュア領域ＤＬＡＰ管理テーブル４１６に記述されているものと同じもの）を設定する。

このとき、セキュア領域ＤＬＡＰ用の特定番号に空きが無ければ、この特定番号を使用しているインストール済みのＡＰをセキュア領域５１のデータ退避領域

５１１に退避させて、空きを作る。

【００５５】

次いで、ＩＣコマンド処理部１３は、インストール処理を行い、作成したデータをデータ格納領域４１２に格納し、ＡＰ管理テーブル４１３にデータアドレスを記述し、インストールフラグをＯＮにする。

このインストール後もセキュア領域５１にＤＬされたＡＰのプログラムコードは、セキュア領域５１のＡＰ保存領域５１２にそのまま存在し、セキュア領域ＤＬＡＰ管理テーブル４１６の記述は残される。そのため、インストールしたＡＰの退避処理に伴ってプログラムコードが削除されても、端末からの再ＤＬは必要が無い。

【００５６】

内部不揮発性メモリへのＤＬを指定するＡＰ（内部不揮発性メモリＤＬ専用ＡＰ）は、セキュア領域への退避を好まない。一方、セキュア領域へのＤＬが可能なＡＰ（セキュア領域ＤＬ可能ＡＰ）は、退避を行うことに問題がないと考えられる。このセキュアカードでは、セキュア領域にＤＬしたＡＰと内部不揮発性メモリにＤＬしたＡＰとを分けて管理しているため、内部不揮発性メモリＤＬ専用ＡＰが格納される領域は、セキュア領域ＤＬ可能ＡＰによって埋められてしまうことはなく、一方、セキュア領域ＤＬ可能ＡＰは、専用の領域が確保されているので、インストール状態にあるセキュア領域ＤＬ可能ＡＰを退避させることで別のセキュア領域ＤＬ可能ＡＰをインストールすることが可能となる。

【００５７】

なお、ＡＰ管理テーブル４１３の分け方は、例えば＃１～＃３は内部不揮発性メモリＤＬ専用ＡＰ向け、＃４～＃５はどちらでもよいＡＰ向け、というような区分でも良い。

また、セキュア領域にＤＬしたＡＰのみを退避可能とし、内部不揮発性メモリにＤＬしたＡＰは退避不可とすることも可能である。この場合には、セキュア領域ＤＬＡＰ管理テーブルの退避可否フラグは無くてもよい。

また、セキュア領域ＤＬＡＰ管理テーブルに、インストールフラグ及びデータ格納アドレスを追加することで、セキュア領域へのインストール（データ格納領

域の生成）を行うこともできる。

【００５８】

ここで示した、内部不揮発性メモリへのＤＬを指定するＡＰには、セキュリティが高いもの、例えば電子マネーＡＰなどが該当するであろう。このような直接金銭に絡む、セキュリティ強度が要求されるＡＰは、内部不揮発性メモリの外にプログラムコード及びデータを出すことが望ましくない。そのため、退避不可と設定されることが考えられる。

【００５９】

また、ＩＣカード（セキュアメモリカードのＩＣ部を含む）の利用が一般に広まるにつれて、厳密な手続きを行わずに任意のプレイヤーがＡＰをカードにインストールすることが可能になるものと考えられる。そうなると、いずれかのサーバにアクセスする際（または、何らかの端末アプリケーションを使用する際）に必要なＩＤとパスワードとを管理するＡＰ等は、セキュア領域ＤＬ可能ＡＰになると考えられる。そのサーバが事業者または個人によって運用される場合（特に個人が運用するサーバの場合）には、さほどセキュリティレベルは要求されず、万一ＩＤとパスワードとを紛失した（壊れた）場合でも、容易に再発行が可能である。

【００６０】

このようなＡＰに対して、電子マネーＡＰと同等に、容量の小さい内部不揮発性メモリを常時利用させることは、コスト面から望ましくない。それよりも、大容量のセキュア領域にＤＬし、同じようにセキュア領域にＤＬしたＡＰを使用する際に退避されるという運用方法が妥当である。

ただ、このような仕分けは、論理必然的に導かれるものではなく、ＡＰ提供者が希望するセキュリティ要求度とカード発行者が判断する内部不揮発性メモリ利用の妥当性とにより様々に設定されることになる。

【００６１】

いずれにしろ、第２の実施形態のセキュアカードでは、セキュア領域へのＤＬが可能であるため、第１の実施形態に比べて、ＡＰのＤＬ処理及びインストール処理における、より多くのパターンが選択できる。そのため、ＡＰの種々のセキ

ュリティ要求レベルに対応することが可能であり、セキュアメモリの秘匿領域を、より効率的に利用することができる。

【００６２】

また、さらに、ＡＰのセキュア領域へのＤＬとともに、セキュア領域へのインストール処理を可能にすれば、ＡＰのＤＬ処理及びインストール処理におけるパターンは一層増加し、セキュアメモリの秘匿領域をさらに効率的に利用することができる。例えば、内部不揮発性メモリにＤＬされ、内部不揮発性メモリにインストール処理された高度セキュリティのＡＰと、セキュア領域にＤＬされ、内部不揮発性メモリにインストール処理された準高度セキュリティのＡＰとを退避不可とし、セキュア領域にインストール処理されたＡＰを退避可とすることなども可能になる。

【００６３】

（第３の実施形態）

本発明の第３の実施形態では、ＡＰ間で共用するデータが退避中である場合のデータの利用について説明する。

ＡＰ間でデータの共有が可能な仕組みを持ち、ＡＰ２が許可したＡＰ（ここではＡＰ１）は、ＡＰ２のデータを参照することが可能であるものとする。許可対象ＡＰ（ＡＰ１）は、許可する側のＡＰ（ＡＰ２）により管理されたデータのうち、特定のデータ（一部のデータ）に対してのみ参照することが可能であり、また、そのような一部のデータに対する他ＡＰからの参照許可を複数設定することが可能であるものとする。

【００６４】

図２６（ａ）には、あるＡＰが参照許可を与えたデータと許可対象ＡＰとの関係を記述した許可指定テーブルの例を示しており、ここでは、図２６（ｂ）に示すように、ＡＰ１に対してｄａｔａ_ａの参照許可が設定されているものとする。また、図１８、図１５（ｆ）及び図１６（ｂ）に示すように、ＡＰ１がインストール状態、ＡＰ２が退避状態とする。

【００６５】

ＩＣコマンド処理部１３は、ＡＰ２の退避処理において、データの退避時に許

可対象のデータｄａｔａ_ａも含めて退避させる。ＡＰ１の実行時に、ＡＰ２が保持するデータｄａｔａ_ａへの参照が発生すると、ＩＣコマンド処理部１３は、ＡＰ管理テーブル（図１５（ｆ））よりＡＰ２がインストール状態にないことを認識し、退避ＡＰ管理テーブル（図１６（ｂ））よりＡＰ２が退避状態であることを認識し、退避中のＡＰ２の暗号化データｅｖａｃ２を読み出し、復号化と署名検証とを行い、検証が正常に終了すれば、復号化したＡＰ２のデータからｄａｔａ_ａを参照する。

【００６６】

また、ｄａｔａ_ａへの書き込みが発生する場合は、更新したｄａｔａ_ａとともにＡＰ２のデータ全体に対して暗号化、署名生成を行い、暗号化データのセキュア領域への格納とともに、格納先を示すｅｖａｃ２を更新し、署名データｓｉｇｎ２を、生成した署名データに更新する。

また、データと同様に、退避中のＡＰのプログラムコードを他のＡＰで利用することも可能である。図２７（ａ）（ｂ）には、あるＡＰが実行許可を与えるプログラムコードと許可対象ＡＰとの関係を記述した許可指定テーブルの例を示している。前述するデータと同様の手順で、ＡＰ１は、退避中のＡＰ２のｃｏｄｅ_ａを実行することができる。

【００６７】

なお、第１の実施形態で示したように、ＡＰの退避には、

①データのみ退避＋プログラム削除

②データ＋プログラムをともに退避

③データのみ退避、プログラムを内部不揮発性メモリに残す

の３パターンがある。第２の実施形態でセキュア領域ＤＬ可能ＡＰに該当するものとして示したサーバへのアクセスに利用するＡＰの場合、利用時にネットワークに接続されるので、プログラムコードのＤＬが可能であるため、①のパターンが適する（②や③の適用を否定するものではない）。

また、端末ＡＰを使用する際に必要なＩＤとパスワードとを管理するようなＡＰの場合には、常にネットワークに接続されている訳ではないため、②のパターンが適している（③の適用を否定するものではない）。なお、③については、Ａ

Ｐ提供者がプログラムコードの退避を望まない場合に適用し得る。

【００６８】

なお、本発明の実施形態では、大容量不揮発性メモリ５０に、記憶領域として、非認証領域、認証領域及びセキュア領域の３領域を設けた例を示しているが、本発明では、大容量不揮発性メモリ５０に、セキュア領域を備えることが必要であって、その他の領域については問わない。

【００６９】

【発明の効果】

以上の説明から明らかなように、本発明のセキュアカードは、秘匿性を備えた領域を効率的に活用して、多数のＡＰの利用に必要なデータを内部で安全に保持することができる。そのため、認証条件を満たす端末であれば、どの端末でも、セキュアカードに保持されたデータを利用することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリの構成を示す図

【図２】

本発明の第１の実施形態におけるセキュアカードの概略図

【図３】

本発明の第１の実施形態におけるセキュアカードの構成を示すブロック図

【図４】

本発明の第１の実施形態におけるセキュアカードのＡＰ管理テーブルの構成を示す図

【図５】

本発明の第１の実施形態におけるセキュアカードの退避ＡＰ管理テーブルの構成を示す図

【図６】

本発明の第１の実施形態におけるセキュアカードのセキュア領域の構成を示す図

【図７】

本発明の第１の実施形態におけるセキュアカードの退避シーケンスを示す図（端末からトリガを掛ける場合）

【図８】

本発明の第１の実施形態におけるセキュアカードの退避シーケンスを示す図（カード自身が判断して退避させる場合）

【図９】

本発明の第１の実施形態におけるセキュアカードの退避データ生成手順を示す図

【図１０】

本発明の第１の実施形態におけるセキュアカードの復元シーケンスを示す図（端末から復元トリガを掛ける場合）

【図１１】

本発明の第１の実施形態におけるセキュアカードの復元シーケンスを示す図（カード自身が自動で復元する場合）

【図１２】

本発明の第１の実施形態におけるセキュアカードの復元データ生成手順を示す図

【図１３】

本発明の第１の実施形態におけるセキュアカードのＡＰ管理テーブルの推移を示す図（ａ～ｃ）

【図１４】

本発明の第１の実施形態におけるセキュアカードのＡＰ管理テーブルの推移を示す図（ｄ～ｅ）

【図１５】

本発明の第１の実施形態におけるセキュアカードのＡＰ管理テーブルの推移を示す図（ｆ～ｈ）

【図１６】

本発明の第１の実施形態におけるセキュアカードの退避ＡＰ管理テーブルの推

移を示す図

【図１７】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その１）

【図１８】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その２）

【図１９】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その３）

【図２０】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その４）

【図２１】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その５）

【図２２】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その６）

【図２３】

本発明の第１の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その７）

【図２４】

本発明の第２の実施形態におけるセキュアカードのセキュア領域の構成を示す図

【図２５】

本発明の第２の実施形態におけるセキュアカードのＡＰ管理テーブルの構成を示す図

【図２６】

本発明の第３の実施形態におけるセキュアカードのデータ参照許可指定テーブルを示す図

【図２７】

本発明の第３の実施形態におけるセキュアカードのコード使用許可指定テーブルを示す図

【符号の説明】

１０　セキュアメモリカード
１１　ＩＣ部
１２　Ｉ／Ｆ部
１３　ＩＣコマンド処理部
１４　ファイル管理部
１５　ＩＣ認証部
１６　メモリ管理部
１７　暗復号回路
１８　内部不揮発性メモリＩ／Ｆ部
２０　制御部
２１　データＩ／Ｆ部
２２　コマンドＩ／Ｆ部
２３　制御認証部
２４　コマンド処理部
２５　アクセス制御部
２６　大容量不揮発性メモリＩ／Ｆ部
４０　ＴＲＭ
４１　内部不揮発性メモリ
５０　大容量不揮発性メモリ
５１　セキュア領域
５２　認証領域
５３　非認証領域
６０　外部ＣＰＵ

４１１　ＡＰ格納領域

４１２　データ格納領域

４１３　ＡＰ管理テーブル

４１４　退避ＡＰ管理テーブル

４１５　鍵管理領域

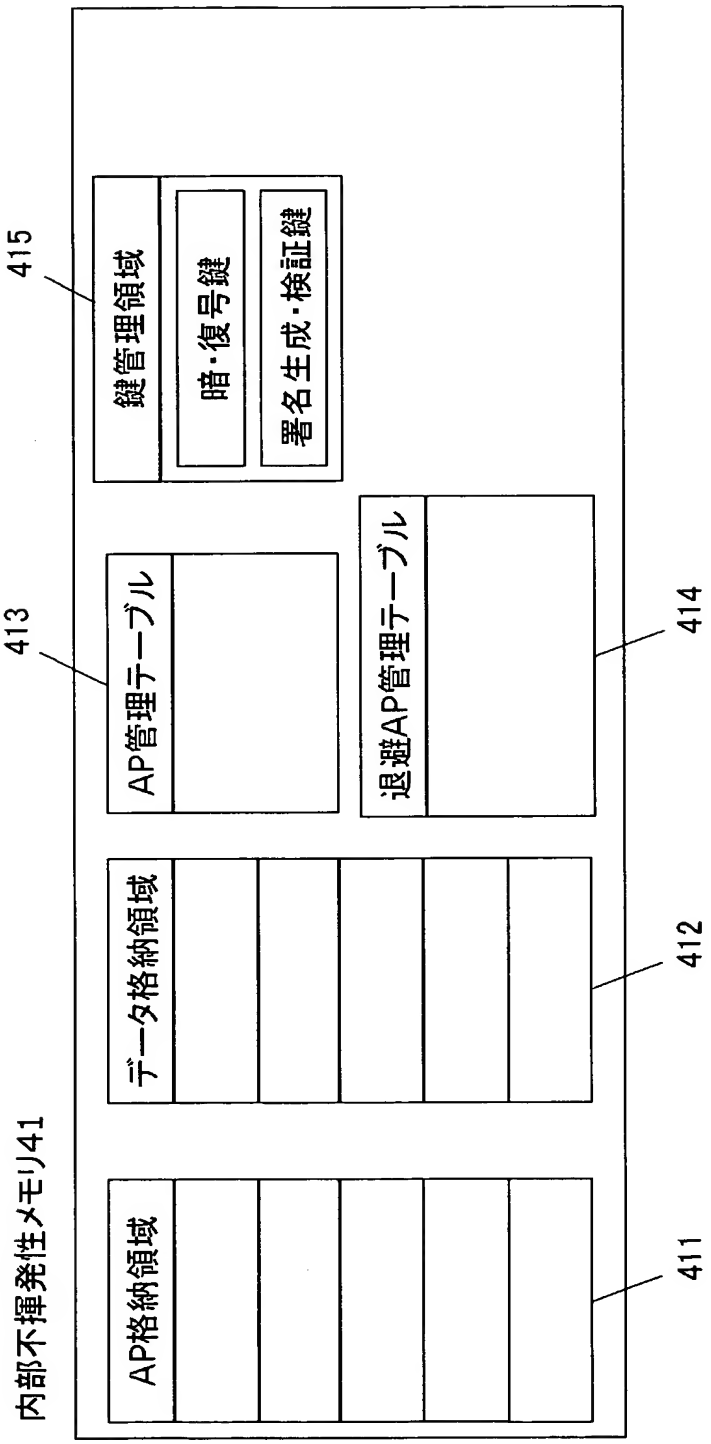
４１６　セキュア領域ＤＬＡＰ管理テーブル

５１１　データ退避領域

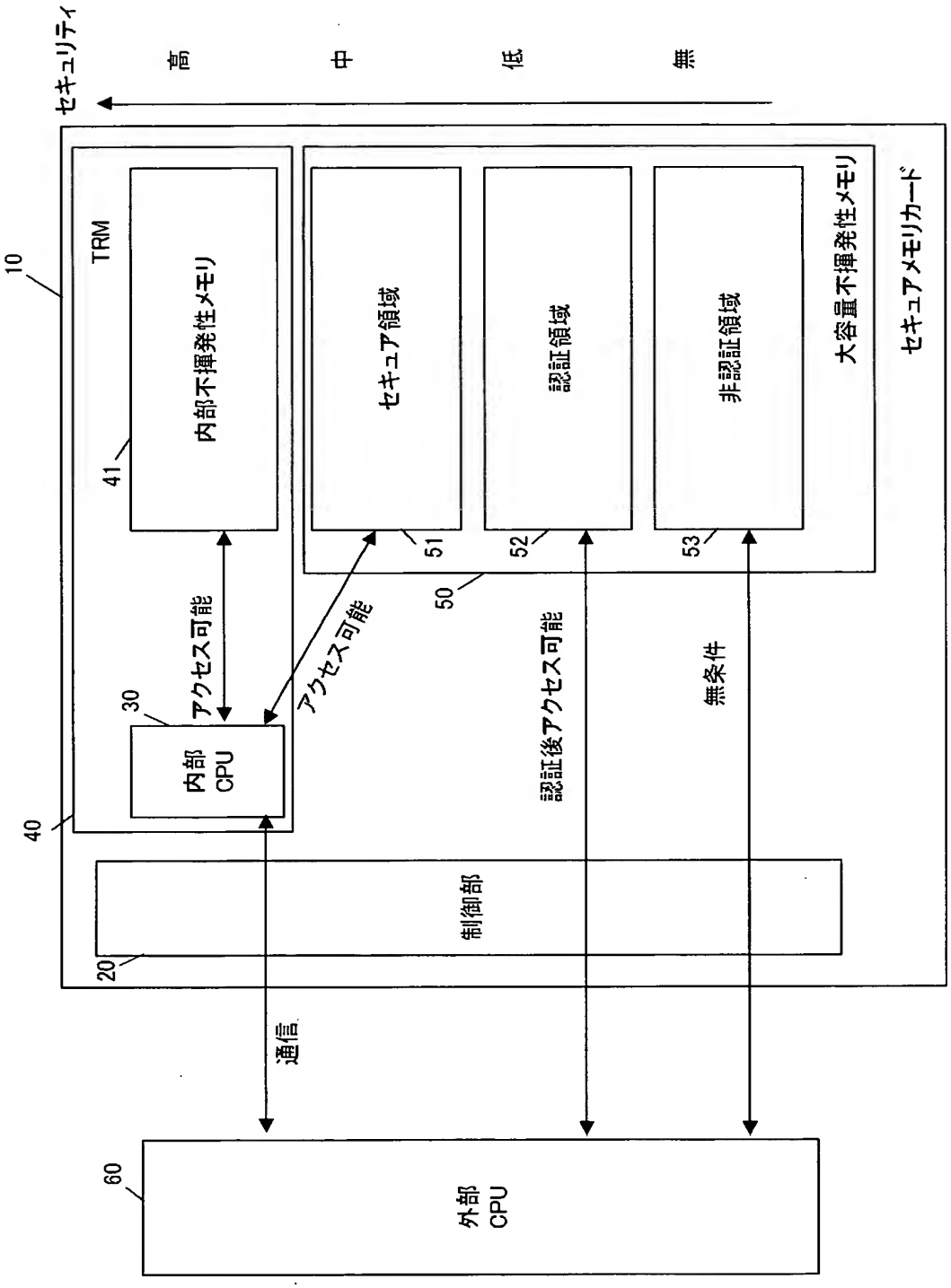
５１２　ＡＰ保存領域

【書類名】　図面

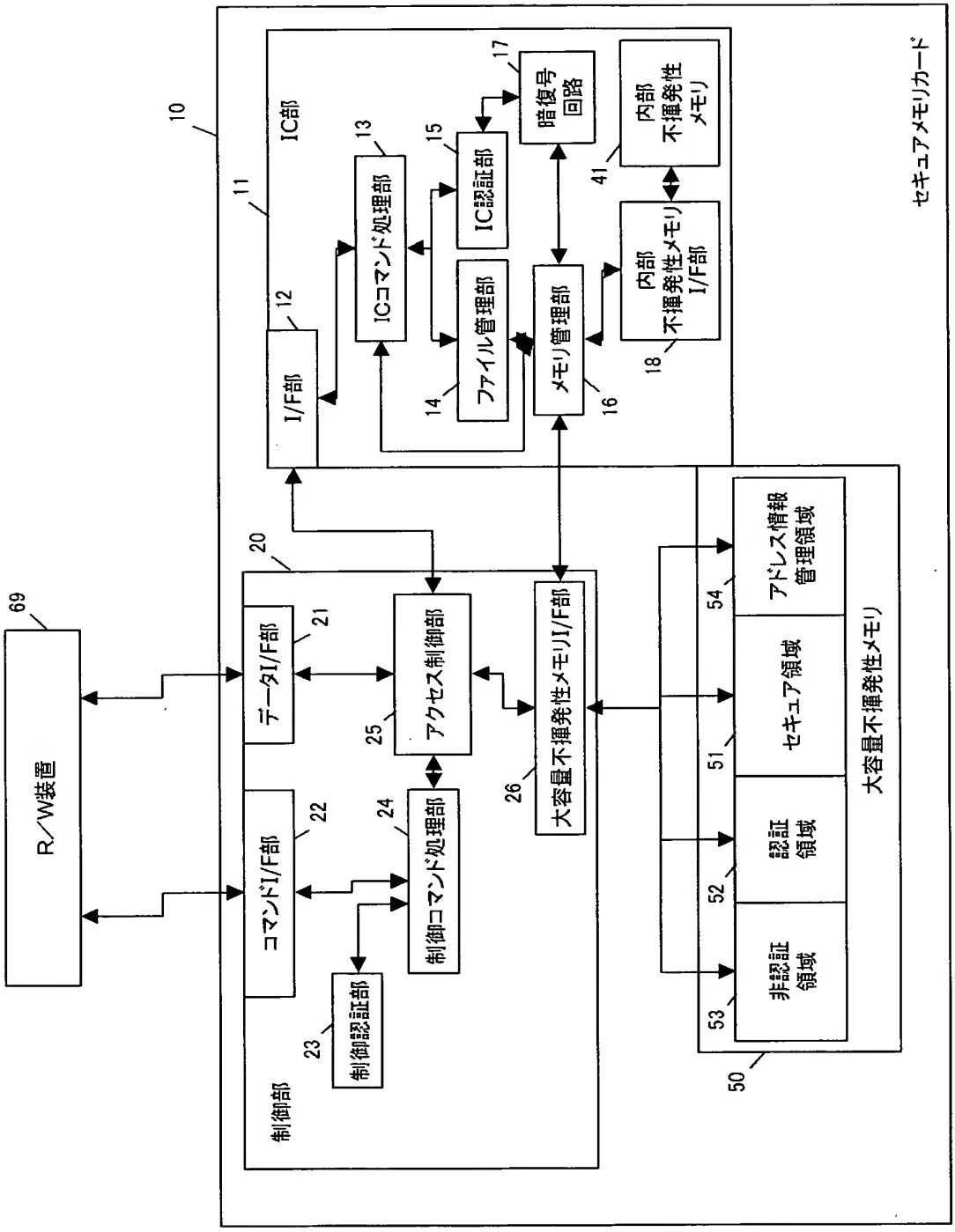
【図１】


内部不揮発性メモリ41
AP格納領域
データ格納領域
AP管理テーブル
退避AP管理テーブル
鍵管理領域
暗・復号鍵
署名生成・検証鍵
411
412
413
414
415

【図２】


セキュリティ
高
中
低
無
10
TRM
内部不揮発性メモリ
41
セキュア領域
認証領域
非認証領域
大容量不揮発性メモリ
セキュアメモリカード
51
52
53
50
アクセス可能
アクセス可能
30
内部CPU
認証後アクセス可能
無条件
40
制御部
20
通信
60
外部CPU

【図３】


R／W装置
69
セキュアメモリカード
10
IC部
11
I/F部
12
ICコマンド処理部
13
IC認証部
15
暗復号回路
17
ファイル管理部
14
メモリ管理部
16
内部不揮発性メモリI/F部
18
内部不揮発性メモリ
41
20
データI/F部
21
コマンドI/F部
22
制御コマンド処理部
24
制御認証部
23
制御部
アクセス制御部
25
大容量不揮発性メモリI/F部
26
大容量不揮発性メモリ
アドレス情報管理領域
54
セキュア領域
51
認証領域
52
非認証領域
53
50

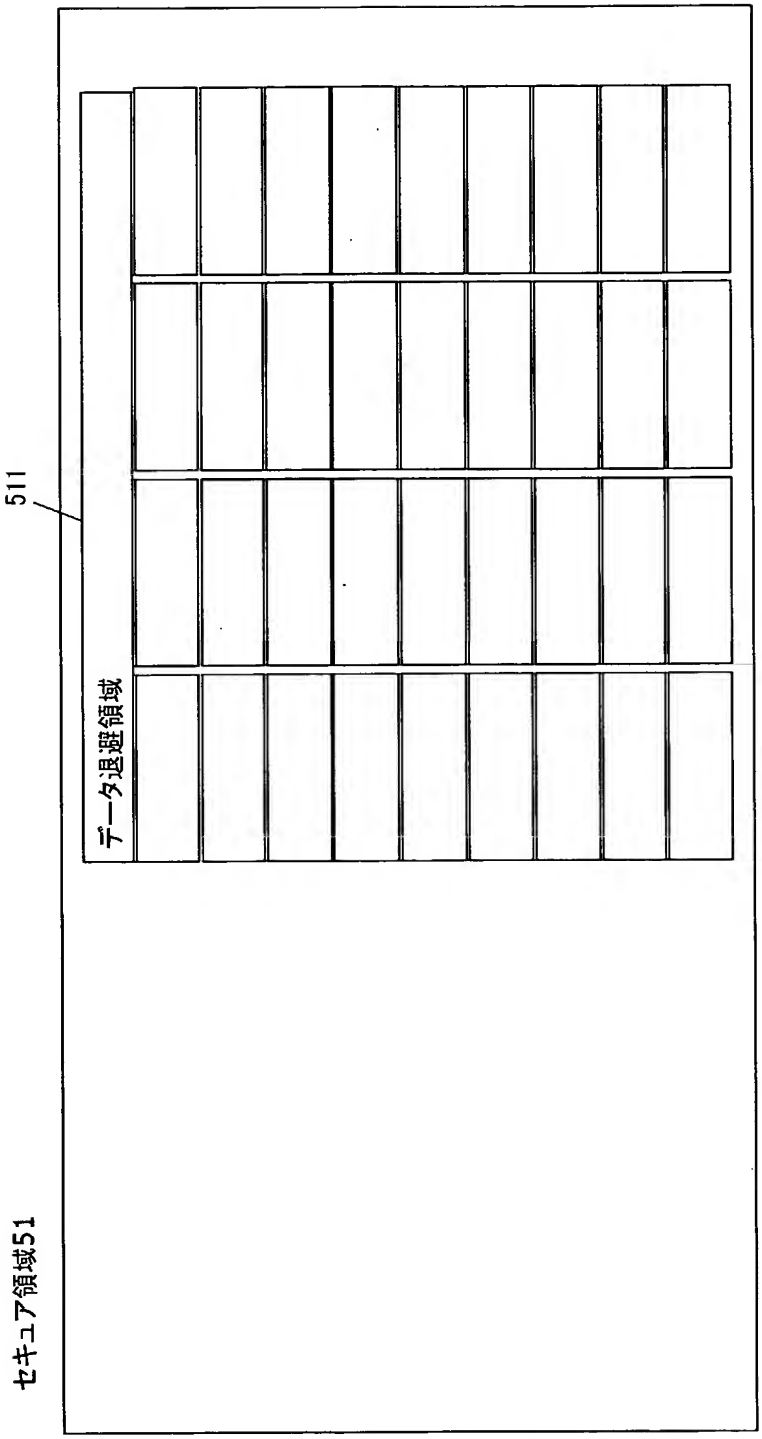
【図４】

#1	AP識別子	インストールフラグ	コードアドレス	データアドレス	退避可否
#2	AP識別子	インストールフラグ	コードアドレス	データアドレス	退避可否
#3	AP識別子	インストールフラグ	コードアドレス	データアドレス	退避可否
#4	AP識別子	インストールフラグ	コードアドレス	データアドレス	退避可否
#5	AP識別子	インストールフラグ	コードアドレス	データアドレス	退避可否

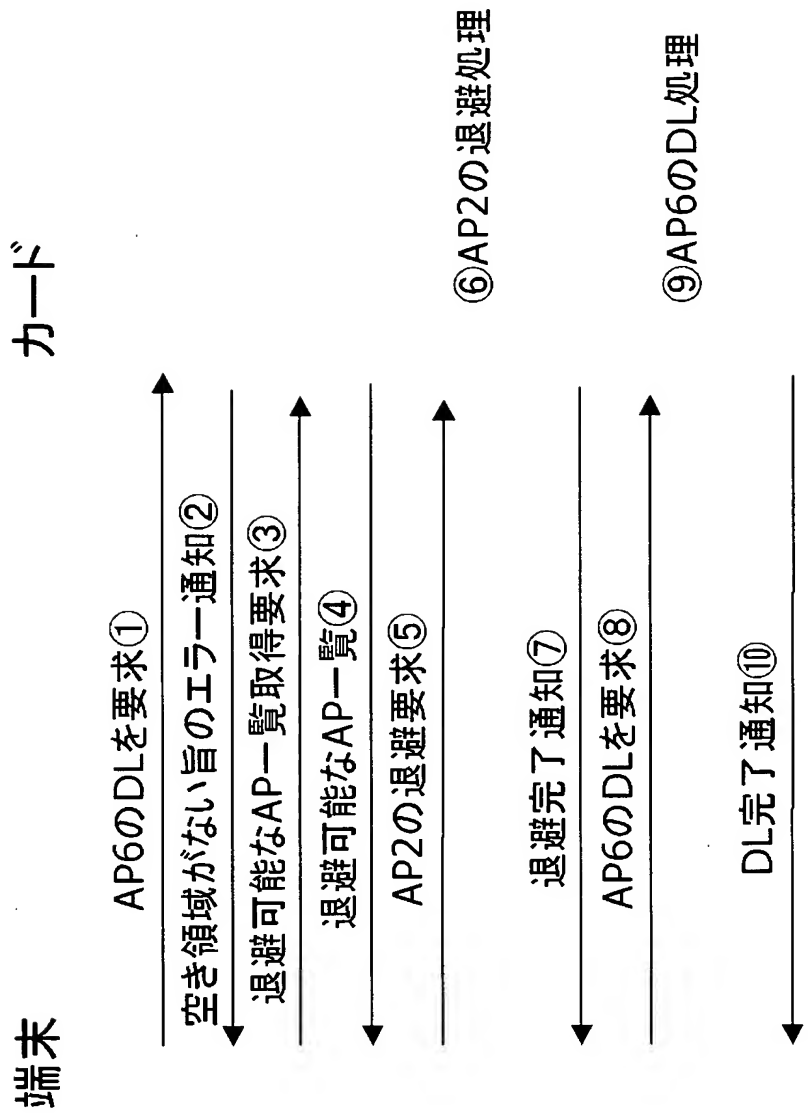
【図５】

AP識別子	退避データ識別子	署名データ
AP識別子	退避データ識別子	署名データ
AP識別子	退避データ識別子	署名データ
AP識別子	退避データ識別子	署名データ

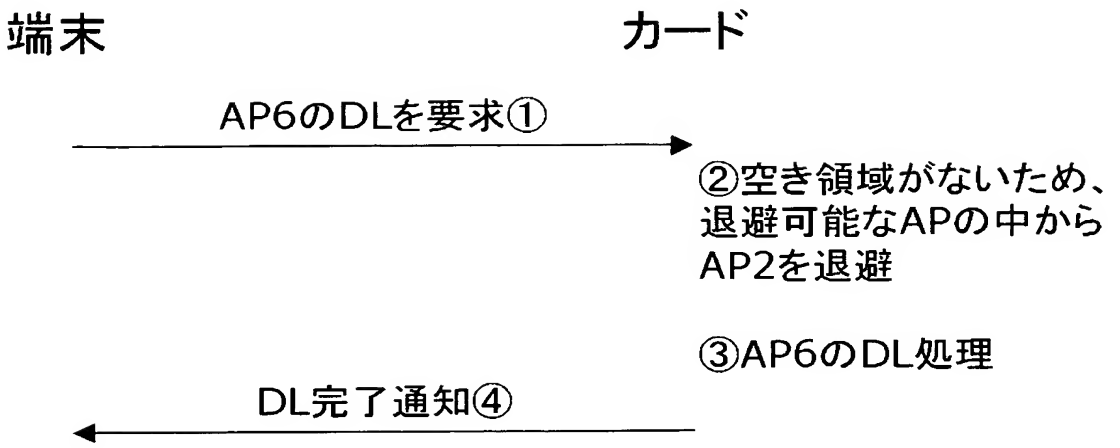
【図６】



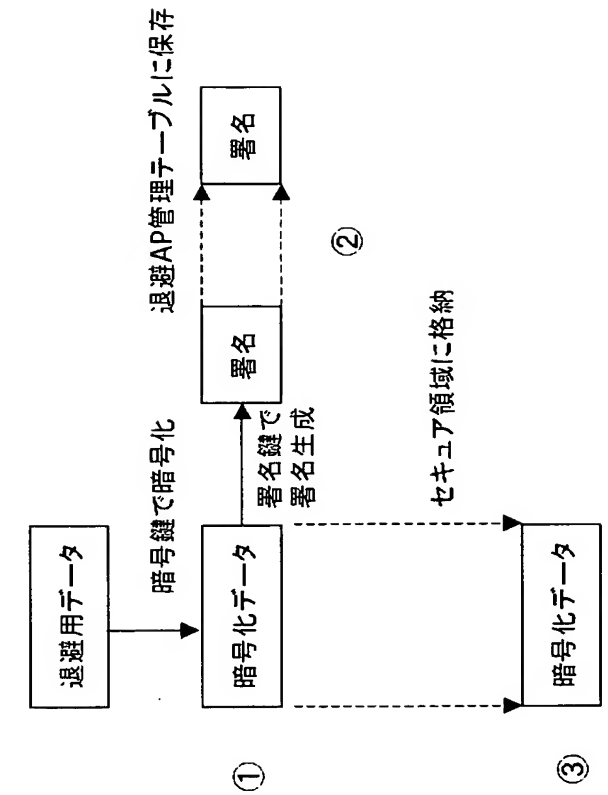
【図７】

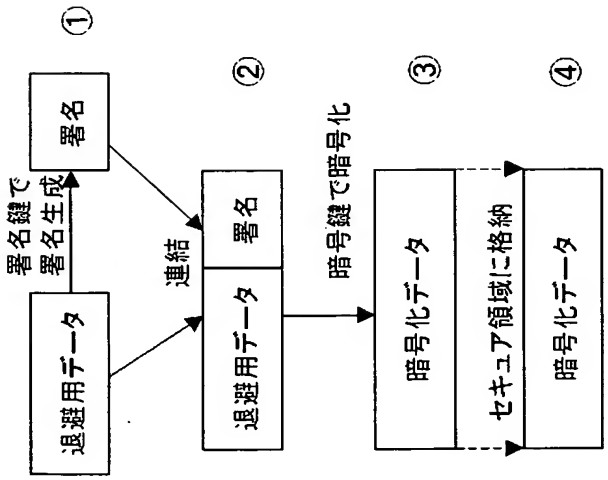

端末
カード
AP6のDLを要求①
空き領域がない旨のエラー通知②
退避可能なAP一覧取得要求③
退避可能なAP一覧④
AP2の退避要求⑤
⑥AP2の退避処理
退避完了通知⑦
AP6のDLを要求⑧
⑨AP6のDL処理
DL完了通知⑩

【図８】

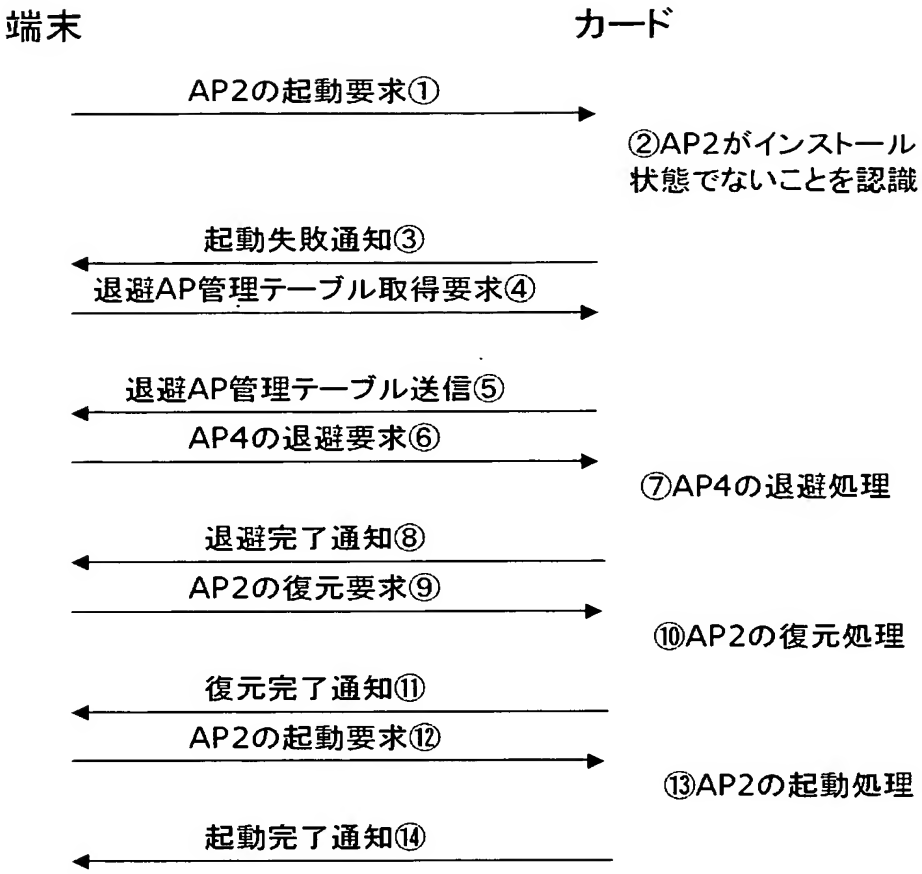

端末
カード
AP6のDLを要求①
②空き領域がないため、
退避可能なAPの中から
AP2を退避
③AP6のDL処理
DL完了通知④

【図９】

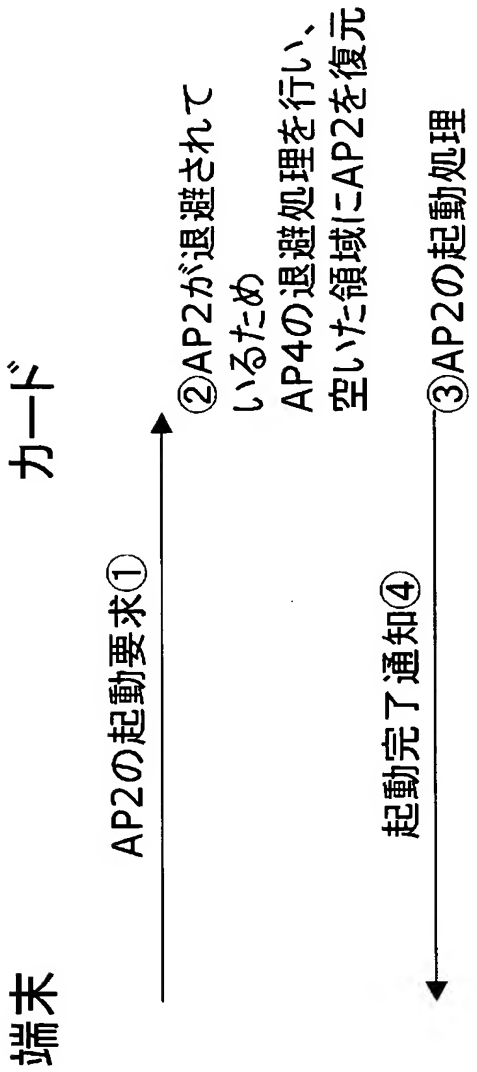

退避用データ
暗号鍵で暗号化
暗号化データ
署名鍵で
署名生成
署名
退避AP管理テーブルに保存
署名
セキュア領域に格納
暗号化データ
①
②
③
(b)


①
②
③
④
署名鍵で
署名生成
署名
退避用データ
連結
署名
退避用データ
暗号鍵で暗号化
暗号化データ
セキュア領域に格納
暗号化データ
(a)

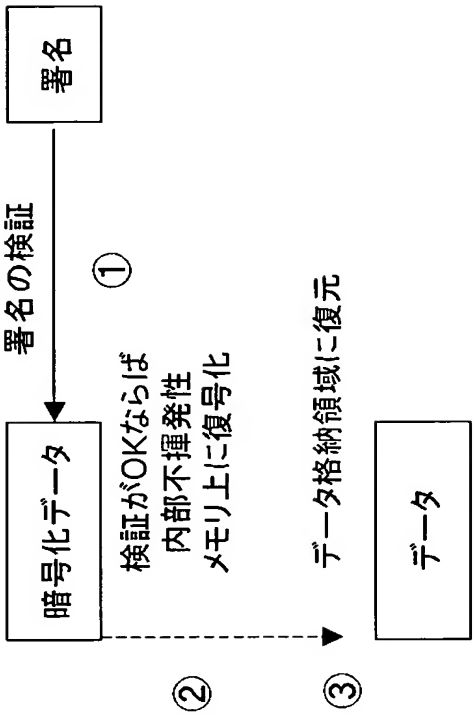
【図１０】


端末
カード
AP2の起動要求①
②AP2がインストール
状態でないことを認識
起動失敗通知③
退避AP管理テーブル取得要求④
退避AP管理テーブル送信⑤
AP4の退避要求⑥
⑦AP4の退避処理
退避完了通知⑧
AP2の復元要求⑨
⑩AP2の復元処理
復元完了通知⑪
AP2の起動要求⑫
⑬AP2の起動処理
起動完了通知⑭

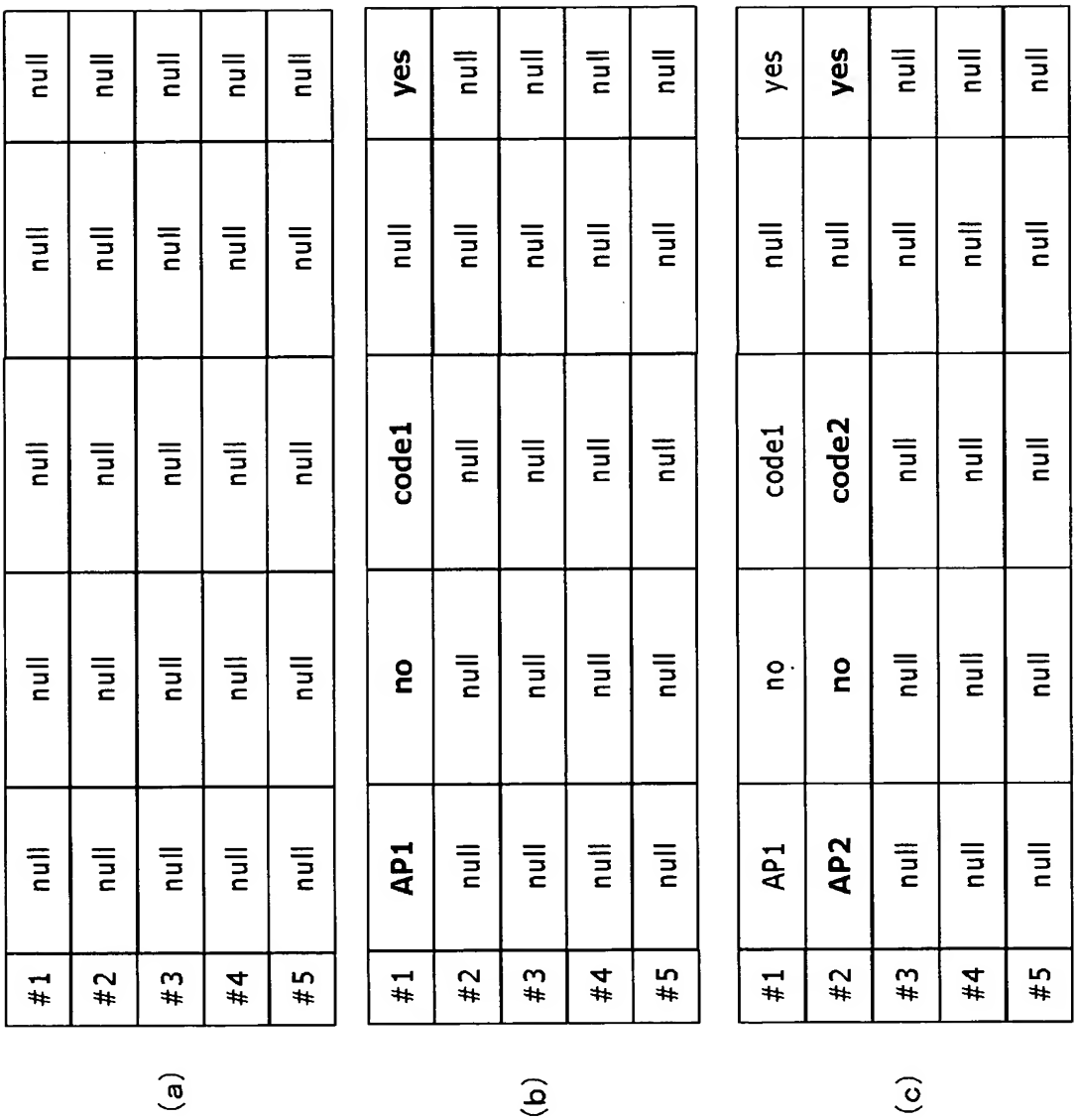
【図１１】


端末
カード
AP2の起動要求①
②AP2が退避されて
いるため
AP4の退避処理を行い、
空いた領域にAP2を復元
③AP2の起動処理
起動完了通知④

【図１２】


署名
署名の検証
①
暗号化データ
検証がOKならば
内部不揮発性
メモリ上に復号化
②
データ格納領域に復元
③
データ
(b)
暗号化データ
内部不揮発性
メモリ上に復号化
①
退避用データ
署名
署名検証
署名検証がOKならば、
退避データをデータ格納領域に復元
②
データ
(a)

【図１３】


(a)
#1 null null null null null
#2 null null null null null
#3 null null null null null
#4 null null null null null
#5 null null null null null
(b)
#1 AP1 no code1 null yes
#2 null null null null null
#3 null null null null null
#4 null null null null null
#5 null null null null null
(c)
#1 AP1 no code1 null yes
#2 AP2 no code2 null yes
#3 null null null null null
#4 null null null null null
#5 null null null null null

【図１４】

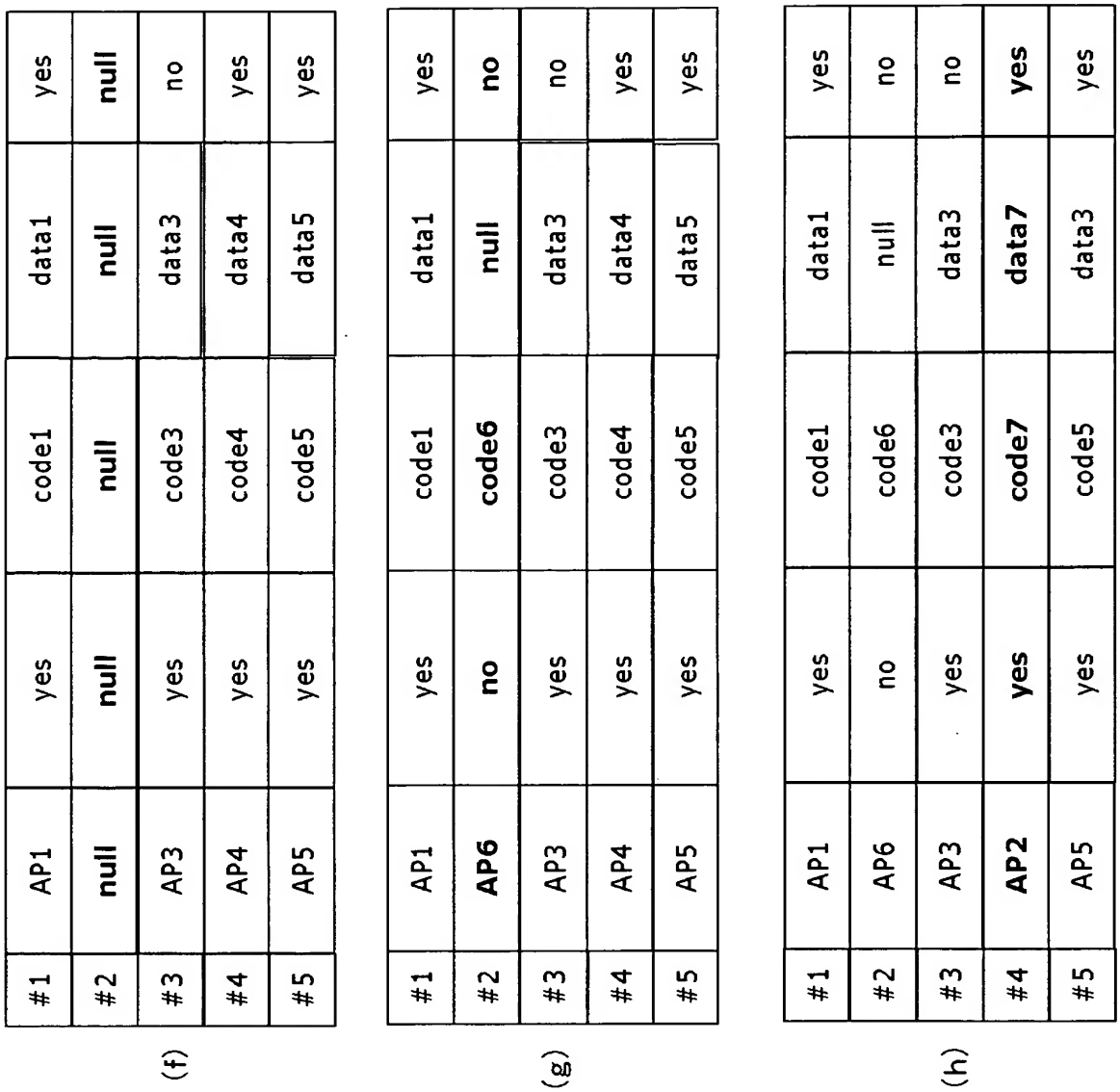
(d)

#1	AP1	**yes**	code1	**data1**	yes
#2	AP2	**yes**	code2	**data2**	yes
#3	null	null	null	null	null
#4	null	null	null	null	null
#5	null	null	null	null	null

(e)

#1	AP1	yes	code1	data1	yes
#2	AP2	yes	code2	data2	yes
#3	**AP3**	**yes**	**code3**	**data3**	**no**
#4	**AP4**	**yes**	**code4**	**data4**	**yes**
#5	**AP5**	**yes**	**code5**	**data5**	**yes**

【図１５】



(f)

#1	AP1	yes	code1	data1	yes
#2	**null**	**null**	**null**	**null**	**null**
#3	AP3	yes	code3	data3	no
#4	AP4	yes	code4	data4	yes
#5	AP5	yes	code5	data5	yes

(g)

#1	AP1	yes	code1	data1	yes
#2	**AP6**	**no**	**code6**	**null**	**no**
#3	AP3	yes	code3	data3	no
#4	AP4	yes	code4	data4	yes
#5	AP5	yes	code5	data5	yes

(h)

#1	AP1	yes	code1	data1	yes
#2	AP6	no	code6	null	no
#3	AP3	yes	code3	data3	no
#4	**AP2**	**yes**	**code7**	**data7**	**yes**
#5	AP5	yes	code5	data3	yes

【図１６】

(a)

null	null	null	null
null	null	null	null
null	null	null	null
null	null	null	null

(b)

AP2	evac2	sign2	
null	null	null	null
null	null	null	null
null	null	null	null

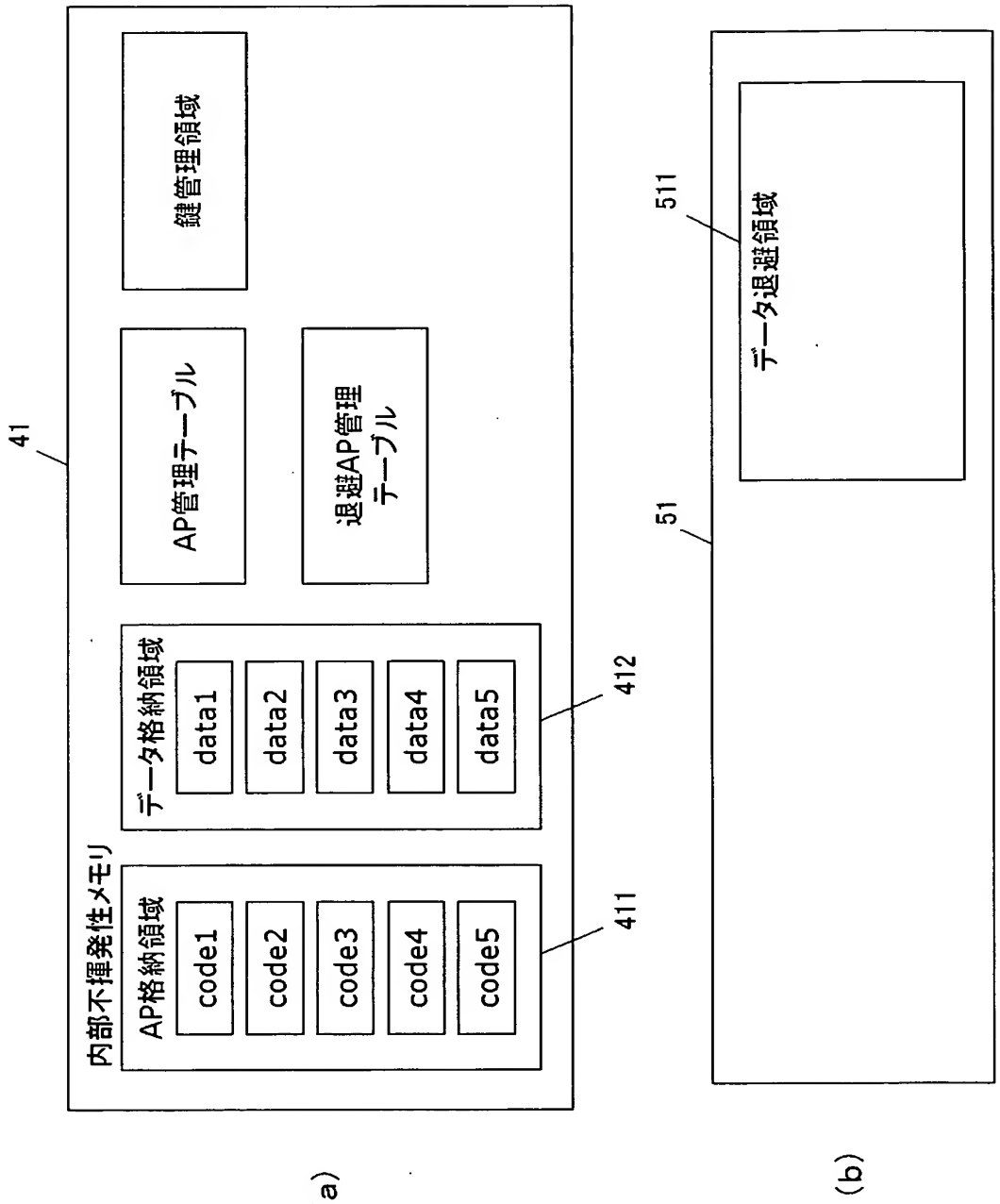
(c)

AP2	evac2	sign2	
AP4	**evac4**	**sign4**	null
null	null	null	null
null	null	null	null

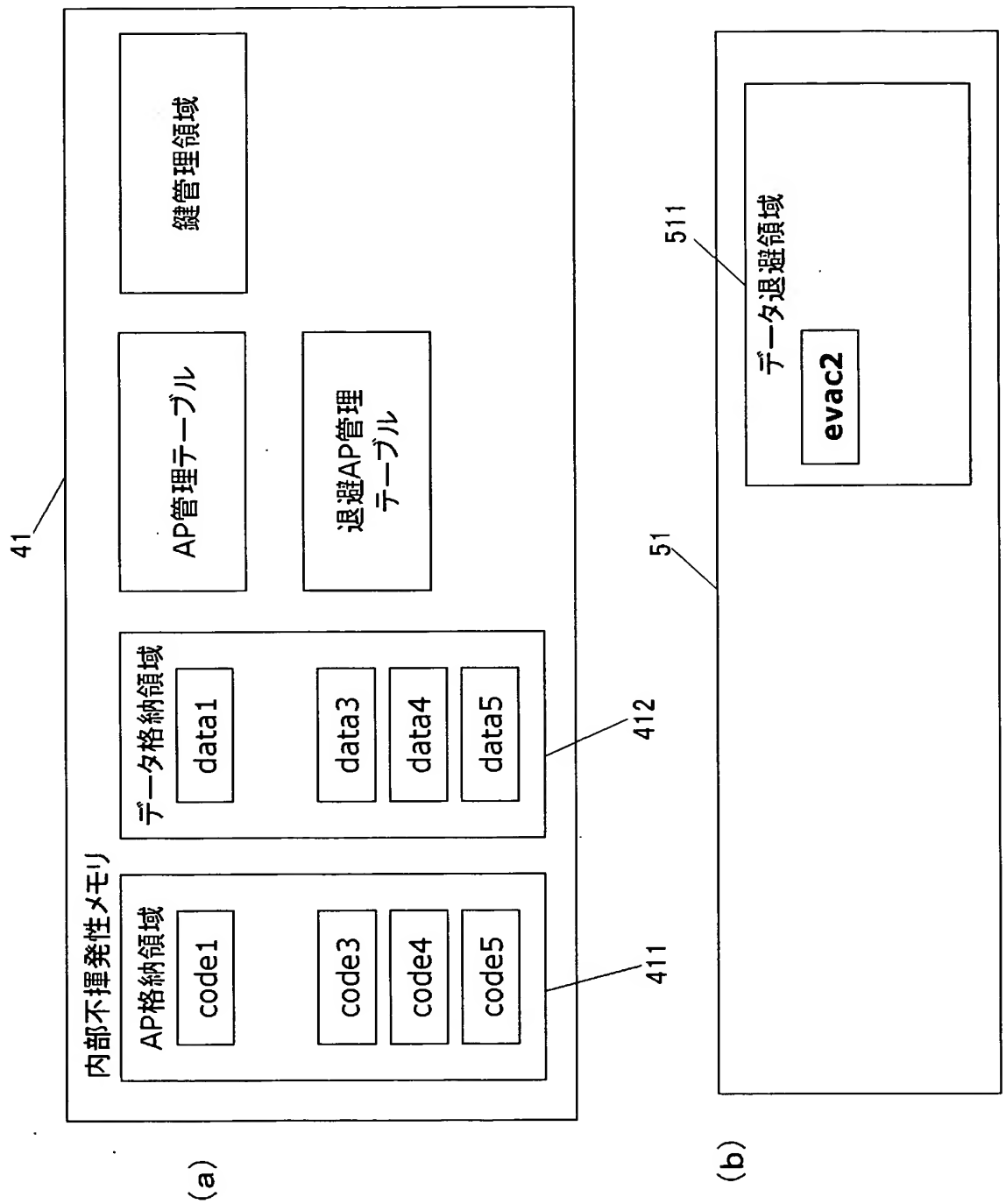
(d)

null	null	null	
AP4	**evac4**	**sign4**	null
null	null	null	null
null	null	null	null

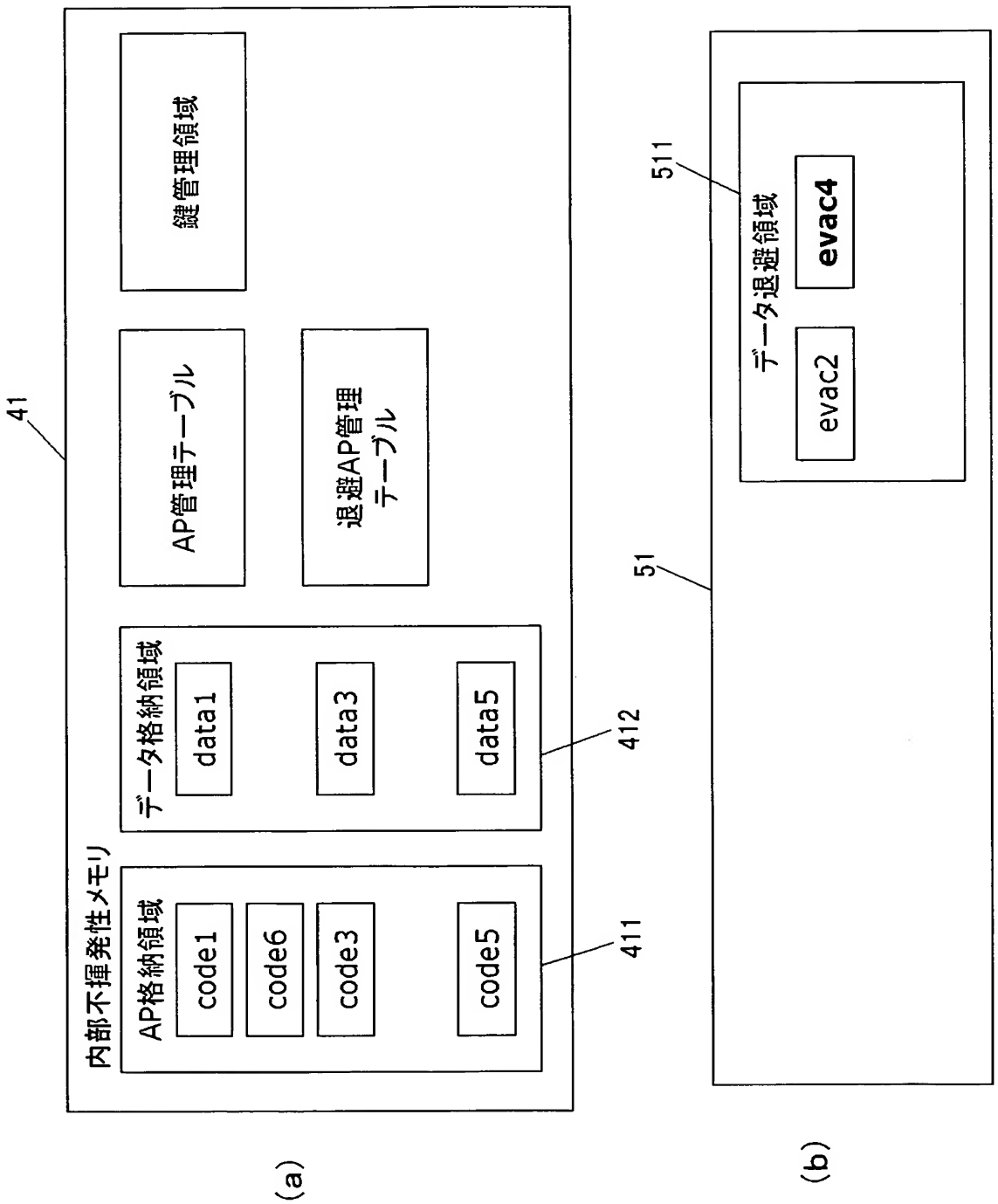
【図１７】


41
内部不揮発性メモリ
AP格納領域
code1
code2
code3
code4
code5
411
データ格納領域
data1
data2
data3
data4
data5
412
AP管理テーブル
退避AP管理
テーブル
鍵管理領域
(a)
51
511
データ退避領域
(b)

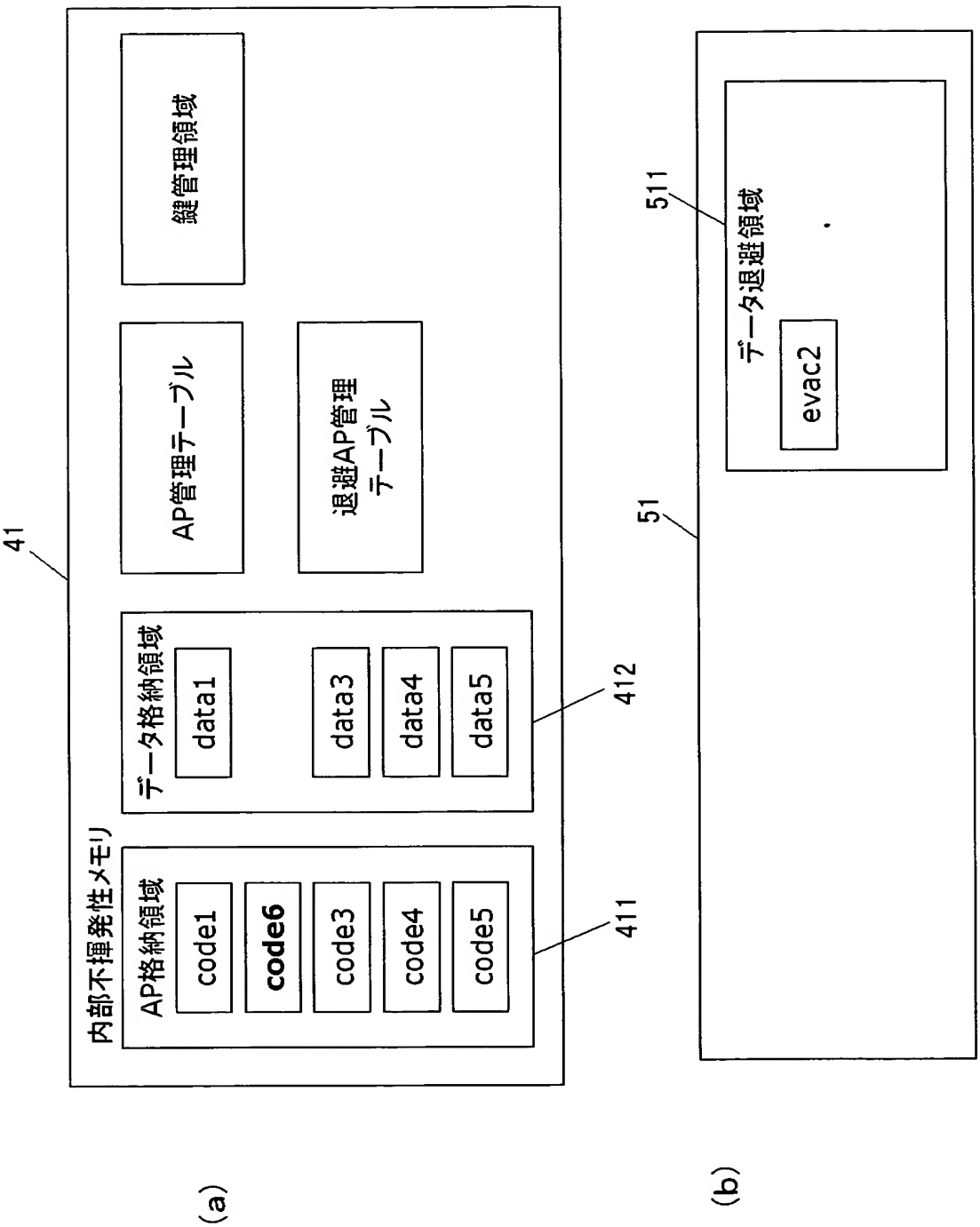
【図１８】


41
鍵管理領域
AP管理テーブル
退避AP管理
テーブル
内部不揮発性メモリ
データ格納領域
data1
data3
data4
data5
412
AP格納領域
code1
code3
code4
code5
411
(a)
51
511
データ退避領域
evac2
(b)

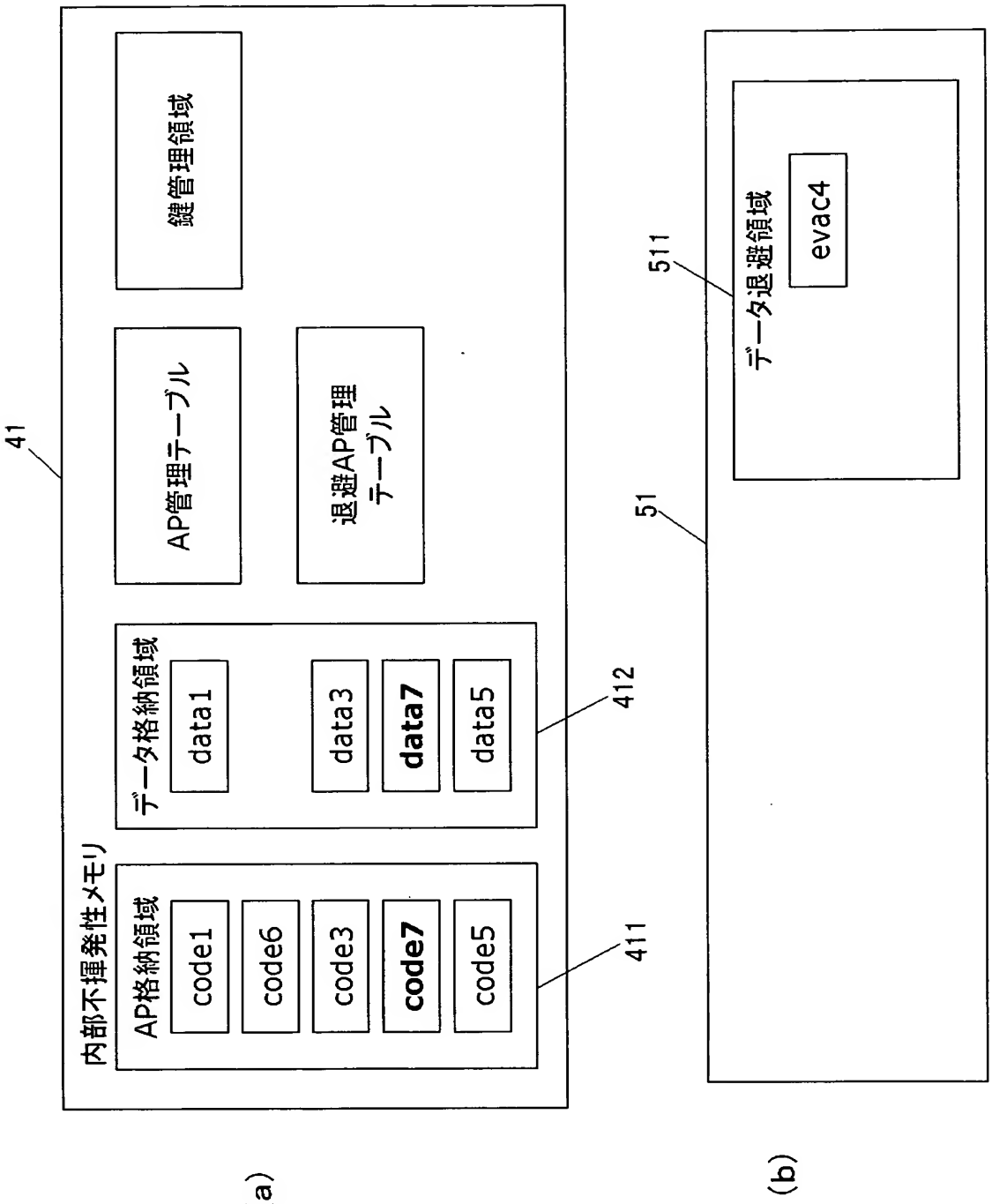
【図１９】


41
鍵管理領域
AP管理テーブル
退避AP管理
テーブル
データ格納領域
data1
data3
data5
412
内部不揮発性メモリ
AP格納領域
code1
code6
code3
code5
411
(a)
51
511
データ退避領域
evac2
evac4
(b)

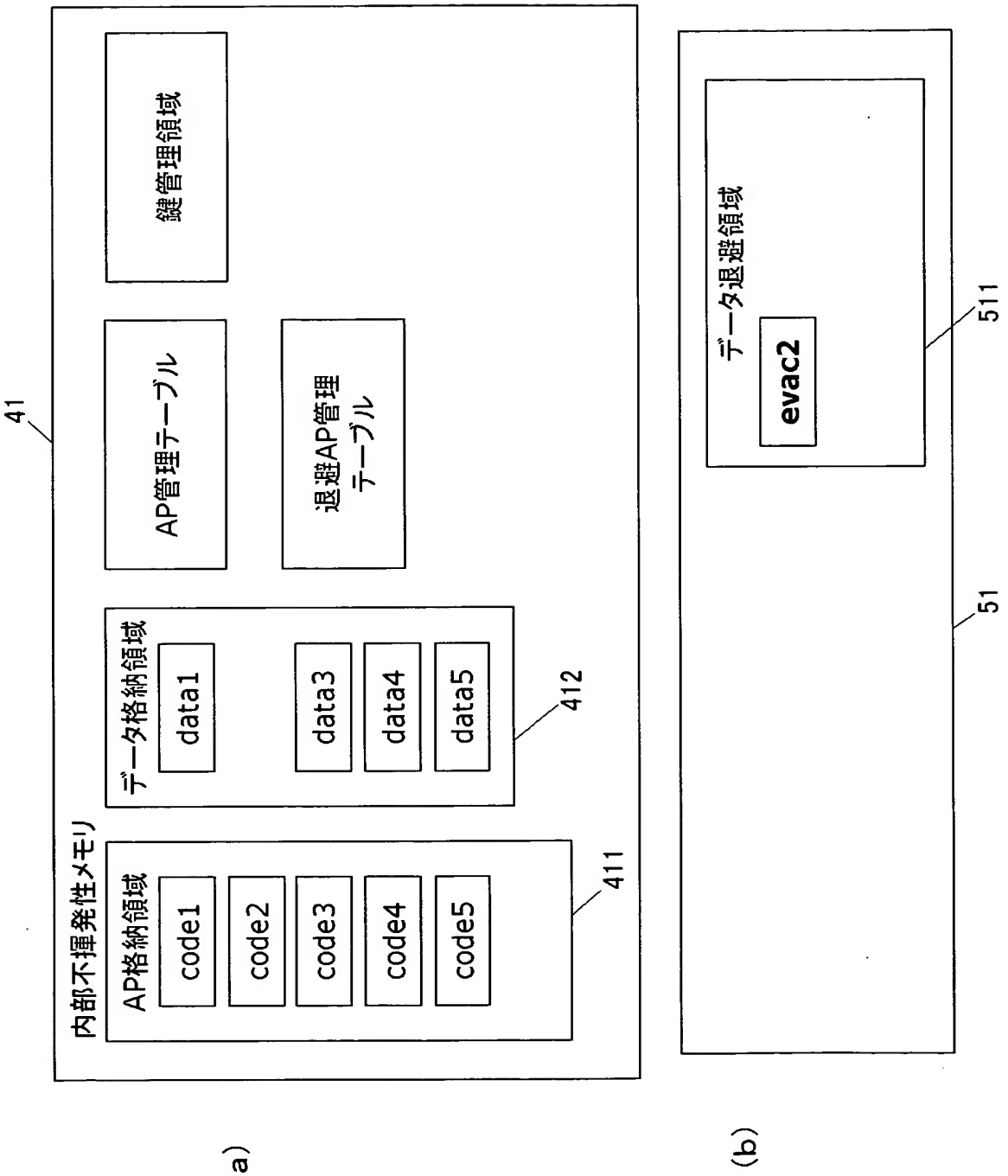
【図２０】


41
内部不揮発性メモリ
AP格納領域
code1
code6
code3
code4
code5
411
データ格納領域
data1
data3
data4
data5
412
AP管理テーブル
退避AP管理
テーブル
鍵管理領域
(a)
51
511
データ退避領域
evac2
(b)

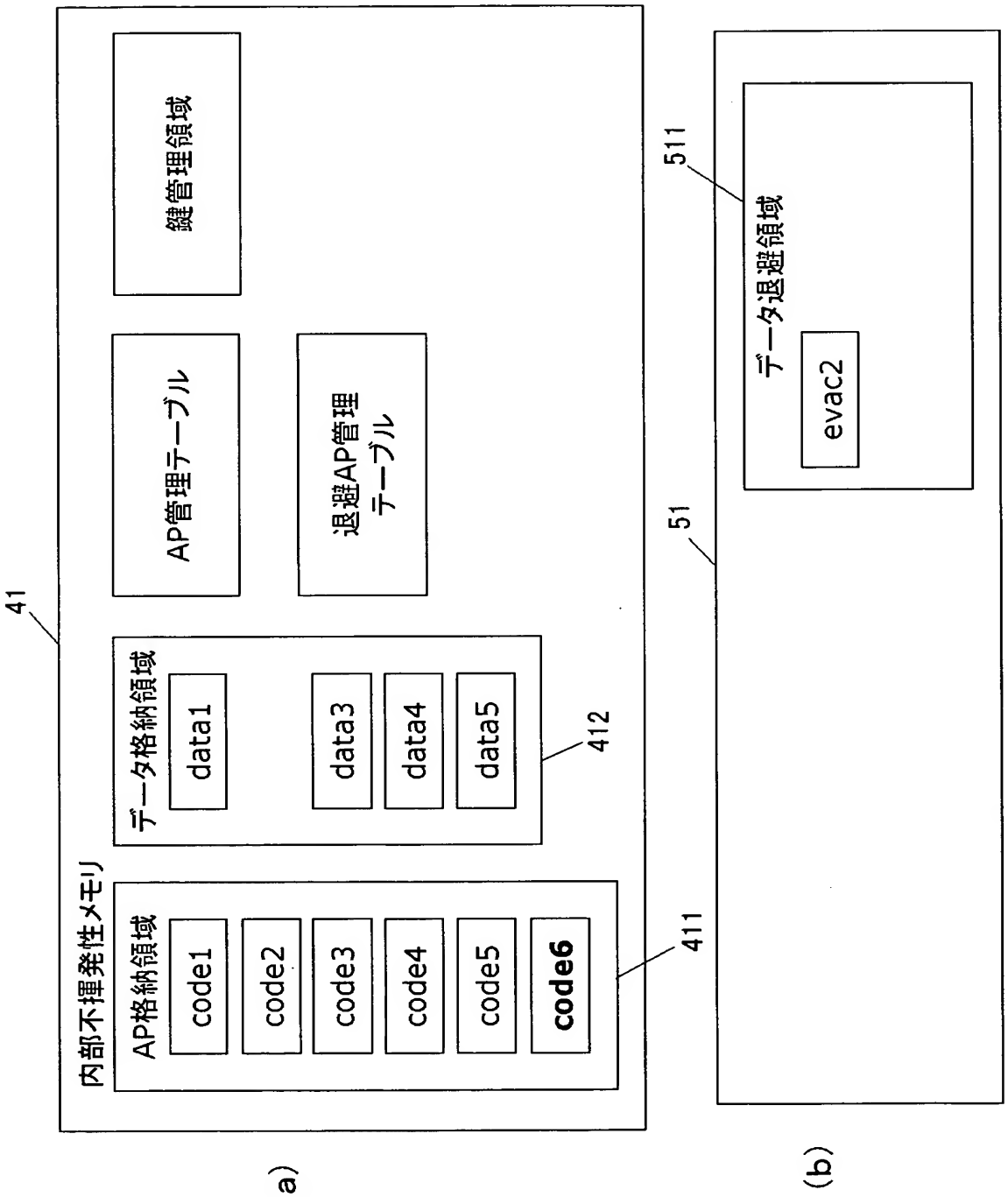
【図２１】


41
鍵管理領域
AP管理テーブル
退避AP管理
テーブル
データ格納領域
data1
data3
data7
data5
412
内部不揮発性メモリ
AP格納領域
code1
code6
code3
code7
code5
411
(a)
511
データ退避領域
evac4
51
(b)

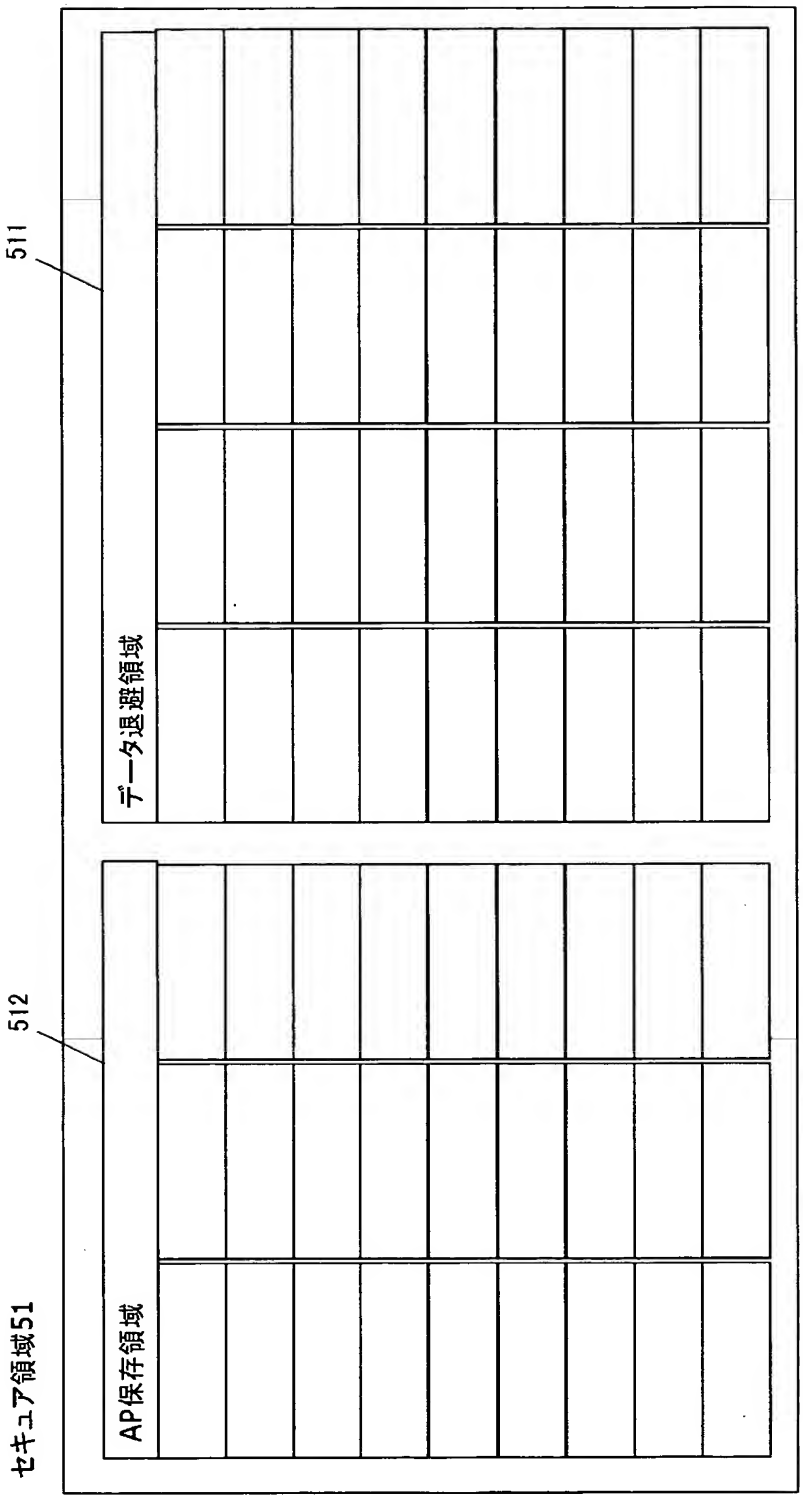
【図２２】


41
鍵管理領域
AP管理テーブル
退避AP管理
テーブル
データ格納領域
data1
data3
data4
data5
412
内部不揮発性メモリ
AP格納領域
code1
code2
code3
code4
code5
411
(a)
51
データ退避領域
evac2
511
(b)

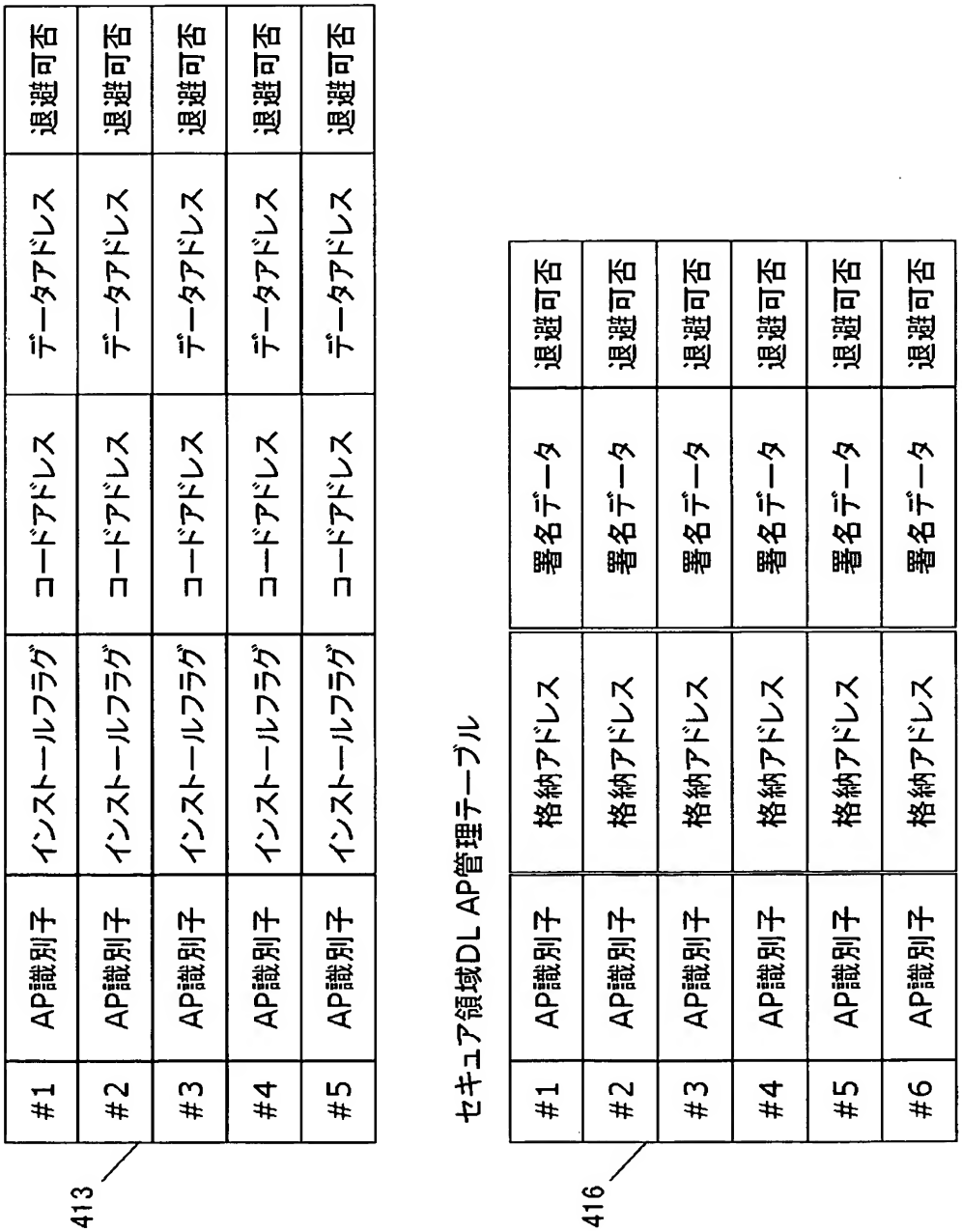
【図２３】


41
鍵管理領域
AP管理テーブル
退避AP管理
テーブル
データ格納領域
data1
data3
data4
data5
412
内部不揮発性メモリ
AP格納領域
code1
code2
code3
code4
code5
code6
411
(a)
51
511
データ退避領域
evac2
(b)

【図２４】



【図２５】


413
#1 AP識別子 インストールフラグ コードアドレス データアドレス 退避可否
#2 AP識別子 インストールフラグ コードアドレス データアドレス 退避可否
#3 AP識別子 インストールフラグ コードアドレス データアドレス 退避可否
#4 AP識別子 インストールフラグ コードアドレス データアドレス 退避可否
#5 AP識別子 インストールフラグ コードアドレス データアドレス 退避可否
セキュア領域DL AP管理テーブル
416
#1 AP識別子 格納アドレス 署名データ 退避可否
#2 AP識別子 格納アドレス 署名データ 退避可否
#3 AP識別子 格納アドレス 署名データ 退避可否
#4 AP識別子 格納アドレス 署名データ 退避可否
#5 AP識別子 格納アドレス 署名データ 退避可否
#6 AP識別子 格納アドレス 署名データ 退避可否
...

【図２６】

許可指定テーブル

(a)

あるAPが管理するデータ全体

データ	許可対象AP
データ	許可対象AP
データ	許可対象AP
・・・	許可対象AP

使用例

(b)

AP2が管理するデータ全体

data_a	AP1
data_b	null
data_c	AP3
・・・	・・・

【図２７】

(a)

許可指定テーブル

あるAPのコード全体

コード	許可対象AP
コード	許可対象AP
コード	許可対象AP
・・・	許可対象AP

(b)

使用例

AP2のコード全体

code_a	AP1
code_b	null
code_c	AP3
・・・	・・・

【書類名】　　要約書

【要約】

【課題】　ＡＰの利用に必要な多くのデータを内部で安全に保持することができるメモリデバイスを提供する。

【解決手段】　電子機器から直接アクセスすることができない耐タンパー性の第１のメモリ４１と、電子機器から直接アクセスすることができない非耐タンパー性の第２のメモリとを設け、第２のメモリを使用して、第１のメモリ４１に蓄積されたデータを退避するように構成している。このメモリデバイスでは、多数のＡＰの利用に必要なデータをデバイス内部で安全に保持することができるため、認証条件を満たす端末であれば、どの端末でも、そこに保持されたデータを利用することができる。

【選択図】　　図１

特願２００３－０４２２８８

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社